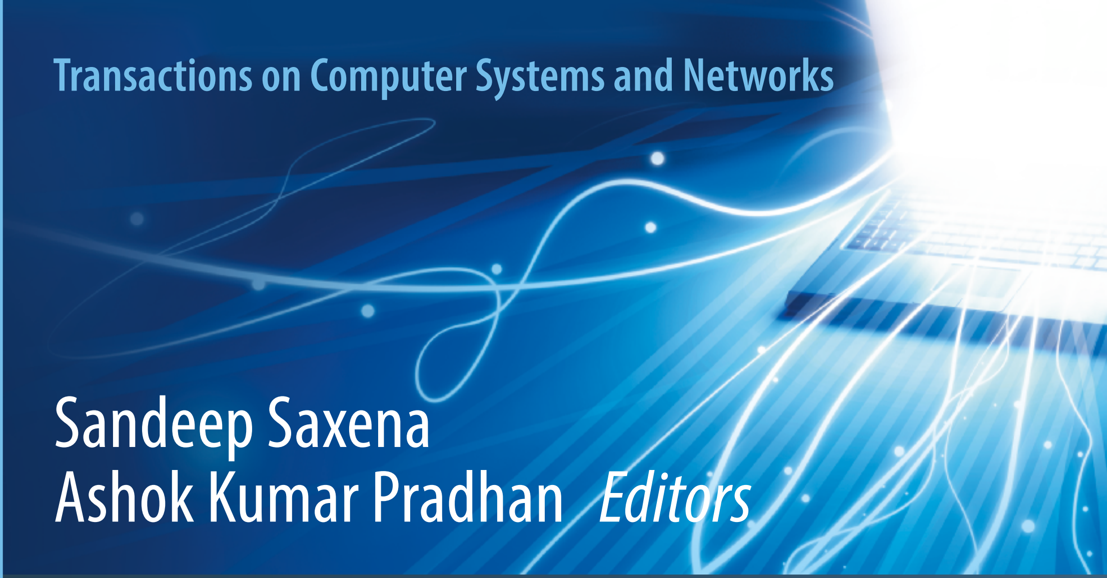


Transactions on Computer Systems and Networks

Sandeep Saxena
Ashok Kumar Pradhan *Editors*

Internet of Things

Security and Privacy in Cyberspace

Springer

Transactions on Computer Systems and Networks

Series Editor

Amlan Chakrabarti, Director and Professor, A. K. Choudhury School of Information Technology, Kolkata, West Bengal, India

Transactions on Computer Systems and Networks is a unique series that aims to capture advances in evolution of computer hardware and software systems and progress in computer networks. Computing Systems in present world span from miniature IoT nodes and embedded computing systems to large-scale cloud infrastructures, which necessitates developing systems architecture, storage infrastructure and process management to work at various scales. Present day networking technologies provide pervasive global coverage on a scale and enable multitude of transformative technologies. The new landscape of computing comprises of self-aware autonomous systems, which are built upon a software-hardware collaborative framework. These systems are designed to execute critical and non-critical tasks involving a variety of processing resources like multi-core CPUs, reconfigurable hardware, GPUs and TPUs which are managed through virtualisation, real-time process management and fault-tolerance. While AI, Machine Learning and Deep Learning tasks are predominantly increasing in the application space the computing system research aim towards efficient means of data processing, memory management, real-time task scheduling, scalable, secured and energy aware computing. The paradigm of computer networks also extends it support to this evolving application scenario through various advanced protocols, architectures and services. This series aims to present leading works on advances in theory, design, behaviour and applications in computing systems and networks. The Series accepts research monographs, introductory and advanced textbooks, professional books, reference works, and select conference proceedings.

More information about this series at https://link.springer.com/bookseries/16657

Sandeep Saxena · Ashok Kumar Pradhan
Editors

Internet of Things

Security and Privacy in Cyberspace

Springer

Editors

Sandeep Saxena
Director-IQAC and Professor-IT
IMS Unison University
Dehradun, Uttarakhand, India

Ashok Kumar Pradhan
Department of Computer Science
and Engineering
SRM University
Amaravati, Andhra Pradesh, India

ISSN 2730-7484 ISSN 2730-7492 (electronic)
Transactions on Computer Systems and Networks
ISBN 978-981-19-1584-0 ISBN 978-981-19-1585-7 (eBook)
https://doi.org/10.1007/978-981-19-1585-7

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Contents

Editors and Contributors

About the Editors

Prof. (Dr.) Sandeep Saxena working as a Director-IQAC and Professor-IT in IMS Unison University, Dehradun, Uttarakhand, India. He has received his Ph.D. degree in CSE from NIT Durgapur, West Bengal. He has received his MS degree in Information Security from the Indian Institute of Information Technology, Prayagraj. He has received his B.Tech degree in CSE from U.P.T.U. Lucknow. He has more than 13 Years of Teaching and Research Experience. His areas of interest and research include Security and Privacy in Blockchain Technology and Cloud Computing, Architecture Design for Cloud Computing, Access control techniques in Cloud Computing, and Blockchain Technology.

He has performed the role of a key member in more than 10 International Conferences as Keynote Speaker/Organizing Secretary/Organizing Chair/Session Chair. He has written 3 technical books for UP Technical University, Lucknow, and published multiple research papers in reputed international journals and conferences. He has published more than 30 research papers in reputed peer-reviewed journals/conferences indexed by (Scopus, SCIE, Google Scholars, DBLP) with high impact factors, more than 10 Patents published, and 2 Patents are Granted. He is participating in multiple professional societies like IEEE (Senior Member), IAASSE (Senior Member), Life Time Member in CSI, and Life Time Member in CRSI.

Ashok Kumar Pradhan is an Associate Professor in the Department of Computer Science and Engineering, School of Engineering and Applied Science at SRM University, Amaravati. He received his M.Tech. degree from the National Institute of Technology (NIT), Rourkela, India, in 2010. He received his Ph.D. degree from NIT Durgapur, India, in 2015. His areas of interest and research include security and privacy in blockchain-based IoT, architecture design for blockchain-based IoT, access control techniques in blockchain-based IoT, blockchain-enabled ecosystem in healthcare, agriculture, and supply chain, experimental prototyping, and testbeds for blockchain-based IoT. He has published over 20 research papers in reputed peer-reviewed journals and conferences. He is a lifetime member of cryptography and security and the Indian science congress association.

Contributors

Pradeep Kumar Arya Department of Computer Science, BML Munjal University, Gurgaon, India

Sunil Kumar Bharti Galgotias College of Engineering and Technology, Greater Noida, India

Prachi Dahiya Delhi Technological University, New Delhi, India

Kunal Das Acharya Prafulla Chandra College, Kolkata, WB, India

Bhaskara Santhosh Egala SRM University, Amaravati, Andhra Pradesh, India

Goldie Gabrani Department of Computer Science and Engineering, BML Munjal University, Gurgaon, India

S. B. Goyal City University, Petaling Jaya, Malaysia

Shubham Gupta Department of Computer Science and Engineering, SRM University, Amravati, Andhra Pradesh, India

Sunil Gupta Department of Cybernetics, School of Computer Science and Engineering, University of Petroleum and Energy Studies, Dehradun, India

Bharathi V. Kalghatgi ECE Department, Pes University, Bangalore, India

Sahil Kansal Galgotias College of Engineering and Technology, Greater Noida, India

Umang Kant Delhi Technological University, Delhi, India

Inderpreet Kaur Galgotias College of Engineering and Technology, Greater Noida, India

Vinod Kumar Delhi Technological University, Delhi, India

Sushma Malik Institution of Innovation in Technology & Management, Janakpuri, New Delhi, India

Yahye Adam Omar City University, Petaling Jaya, Malaysia

Ashok Kumar Pradhan SRM University, Amaravati, Andhra Pradesh, India

Anamika Rana Maharaja Surajmal Institute, Janakpuri, New Delhi, India

Arindam Sadhu Maulana Abul Kalam Azad University of Technology, Kolkata, WB, India;
Greater Kolkata Engineering and Management, Kolkata, WB, India

Sandeep Saxena Director-IQAC and Professor-IT, IMS Unison University, Dehradun, Uttarakhand, India

Rishi Raj Singh School of Computer Science UPES, Dehradun, India

Manish Thakral School of Computer Science UPES, Dehradun, India

Raveena Yadav Delhi Technological University, Delhi, India

Chapter 1
Pre-requisite Concepts for Security and Privacy

Inderpreet Kaur, Sunil Kumar Bharti, and Sandeep Saxena

1.1 Principles of Cryptography

We need to preserve records of everything that happens in our lives. In other words, information could be a valuable asset a bit like the other. Information must be safeguarded against cyber-attacks because it is a valuable asset. In order to be safe, information must be protected against illegal access (confidentiality), protected from unlawful change (integrity), and accessible only to authorize parties when needed (availability) (Failed 2019; Hambouz et al. 2019) (Fig. 1.1).

1.1.1 Confidentiality

The most common feature of information security is confidentiality. We must safeguard our private information. An organization must protect itself against actions that jeopardize the confidentiality of its critical data. Confidentiality of data usually refers to it being known to only approve user data. Confidentiality is an important layer of data security. Control of confidential information is the major worry in the military. The operation of an organization necessitates the concealment of some information from others. It ensures that confidential information can be accessed only by an authorized person and should be reserved away from all those who are not authorized to access them.

I. Kaur · S. K. Bharti
Galgotias College of Engineering and Technology, Greater Noida, India
e-mail: Inderpreet.kaur@galgotiacollege.edu

S. Saxena (✉)
Director-IQAC and Professor-IT, IMS Unison University, Dehradun, Uttarakhand, India
e-mail: sandeep.research29@gmail.com

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_1

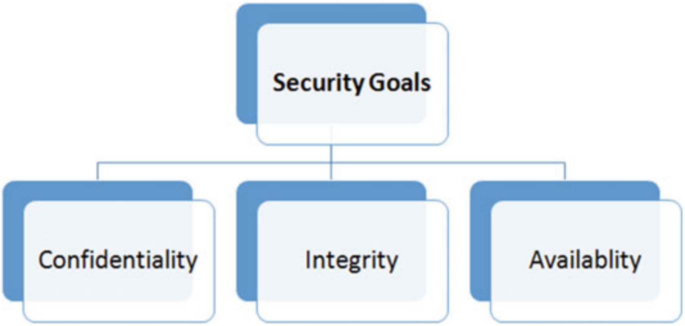


Fig. 1.1 Taxonomy of security goals (https://www.includehelp.com/cryptography/introduction.aspx)

Confidential data means the data can only be accessed by that user only to whom it belongs.

For example, in banking the account details of customer need to be kept undisclosed. Only account holder can view their bank account summary. Only account user is allowed to access the bank account details like bank statement, available balance, etc. Others cannot have right to use these bank details. Hence, this data is called confidential data.

The confidential data have two related concepts, namely data confidentiality and privacy.

Data confidentiality: This phrase ensures that confidential or sensitive information is not disseminated with unauthorized entities.

Privacy: The most popular understanding of privacy evokes feelings of withdrawal, seclusion, secrecy, or being hidden from public view, but without any negative undertone.

A collapse of confidentiality is the illegal confession of information. Confidentiality extends not just to information storage, but also to information transmission. When a piece of information is conveyed, it is referred to as a piece of data. It must be saved on a remote computer, and when data from a remote computer is retrieved, it must be wrapped during transmission.

Confidentiality ensures that no unauthorized users have access to the information shared. Applications, processes, other systems, and/or humans could all be users. When designing a system, make sure there are enough control devices in place to enforce confidentiality, as well as policies that dictate what authorized users can and cannot do with the data. Data must be protected within and outside the automotive, when it is stored (data at rest), sent (data in motion), and processed, in order to maintain confidentiality in automotive systems (data in use). Data in use can be protected with memory protection. Cryptography is excellent at safeguarding the confidentiality of data in transit and at rest, but it adds computational complexity and increases latency; thus, it should be used with caution in time-critical applications.

Confidentiality with Symmetric Encryption

Symmetric encryption is a standard approach for ensuring data confidentiality when it is stored or transmitted. After that, the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES), both block encryption approaches, are used (Martin 2011).

Strong passwords, multifactor authentication, data isolation, encryption, and assigning appropriate user permission levels to clients are just a few of the steps that can be taken to ensure confidentiality. However, before applying such controls, it is critical to divide your information resources into several groups based on the potential for loss if an unauthorized individual contacts them. The stronger the security rights, the greater the negative impact.

The common threats to confidentiality are:

Eavesdropping Attacks

Hackers intercept, destroy, or change data sent between two devices in eavesdropping attacks.

Spy, sometimes known as espionage or tracking, intercepts data transferred between devices across an unsecured network. Eavesdropping occurs when a client connects to an insecure network and transfers confidential business data to a coworker, to give a more thorough description.

Because data is transmitted via an open network, hackers can use a variety of methods to erase it (Ma et al. 2016).

Eavesdropping attacks are notoriously difficult to detect. Errors, unlike other types of network attacks, may not have a substantial influence on the operation of networks and equipment (Tugnait Oct. 2016).

Eavesdropping Methods

Hackers can use a variety of tactics to initiate attacks via eavesdropping. Multiple eavesdropping devices are typically used in these assaults to eavesdrop in conversations and network operations.

A hidden error that is actually installed in a workplace or house is a good example of an electronic eavesdropping device. Bugs may be hidden under a chair or on a table, or the microphone could be hidden in a common object like a bag or a pen. This is a straightforward procedure, but it may result in the installation of equipment that is more difficult to detect.

Although all the technological advances have made digital listening easier and easier, many attacks still rely on capturing phone calls. This is because the phone has electricity, a built-in microphone, hiding hole space, speakers, and it is easy to install holes quickly. An eavesdropper can verify the conversation in the room where the phone is located and call a phone anywhere in the world.

Modern computerized telephone systems can intercept calls electronically without directly touching the equipment. Hackers can send signals through the phone line and listen in any discussion in the same room, even if the phone is not turned on. Similarly, computer systems include advanced communication devices that allow eavesdroppers to collect communication activities such as voice conversations, online chats, and even keyboards to convey what the user is typing.

In addition, computer systems produce electromagnetic radiation, which can be used by sophisticated intruders to rearrange the contents on the computer screen. These signals can travel hundreds of feet and then be pushed out farther using cables and telephone lines as antennas.

Pickup Device

To eavesdrop on the target, an attacker can utilize equipment that collect sound or images, such as microphones and cameras, and convert them to electronic representations. It should ideally be an electrical gadget that consumes the target room's energy so that the attacker does not need to enter the room to charge or replace the battery. Some listening devices have the ability to store digital data and send it to the listening station. Micro-amplifiers can also be used by attackers to reduce background noise.

Transmission Link

Eavesdropping can be done on the transmission link between the device and the attacker's receiver.

This can be accomplished through the use of radio frequency wiring or transmission, for example unused telephone wires, ungrounded wire conduits, or wires. Some transmitters can operate constantly, but more complex methods involve distant enabling.

Listening Station

A listening station is used to relay talks that have been intercepted due to telephone malfunctions.

After you pick up the phone to make or receive a call, the recorder is activated, and it switches off when the call is finished. An attacker can watch, record, or send signals for processing from a listening station, which is a secure location. It can be found just a few blocks away, in the next room or on the phone. Voice-activated equipment will be installed in the monitoring station, allowing it to listen in and record any action.

Weak Passwords

Attackers can easily get unauthorized access to user accounts with weak passwords, giving them access to company systems and networks. Hackers can interrupt secret communication lines, listen in colleagues' activities and chats, and steal confidential or valuable company data.

Open Network

Attackers can easily eavesdrop on users connected to open networks that do not require passwords and do not utilize encryption to send data. Hackers can track user activities and listen in network connections.

Encryption Cracking

Hackers employ encryption cracking tools to break the secrecy by attempting to overcome the network encryption used when delivering data, and data packets can be intercepted. The software's functionality varies depending on the hacker's goals. There are three basic encryption–decryption techniques, each of which decrypts sensitive data in a different way. IT firms in Ottawa can greatly improve network security for all clients and successfully defend against customer threats by understanding these tools (Al-Mohammed et al. 2020).

Traffic Injector

The traffic injector's main function is to inject encrypted communications into a network that have been forged by hackers. For traffic injection, there are two basic objectives. One is to send the recipient a new message, which normally occurs when the hacker has access to the decryption key for the message delivered to the user. Another goal of traffic injection is to retrieve encrypted and plain text messages. After that, the hacking tool compares the two messages to determine their meaning. Airplay and WepWedgie were the two tools employed in the most recent attack (Sala et al. 2021).

Decryption Tools

Decrypting messages usually necessitates the use of two tools. The first tool is used to gather the decryption packets. Today's prominent data packet gathering tools include Wireshark and Prism dump. The second tool examines the collected data packets in order to determine the encryption key. Although the most recent tools use simple algorithmic procedures to decrypt data packets, the tools that collect the data packets are responsible for the majority of the burden. To evaluate and decrypt the key, at least 5 million frames are necessary.

Brute-Force Attack Tools

Brute-force attacks are interested in collecting data packets and attempting to decipher the encrypted code using a large number of key dictionaries stored in it. Until the correct key is found or all keys have been used, the software attempts to decode the data packet with the key. A dictionary-based attack is another name for this type of assault. Decryption takes a lengthy time with brute-force attack methods, ranging from a few days to a few weeks. To function properly, they also necessitate sophisticated CPUs and other resources. The brute-force assault tool Air Snort is widely used (Bhowal et al. 2017).

For example, companies that provide computer services in Ottawa must ensure that their customers are protected against decryption tools by researching them and applying various techniques to ensure that messages carried across the customer's network are not disrupted or modified.

1.1.2 Integrity

Information must be updated on a regular basis. When a client deposits or withdraws money from a bank, the balance of her account must be updated. Changes must be made by authorized individuals and through permitted procedures in order to maintain integrity. Integrity violations are not always the consequence of malevolent behavior; a system disruption, such as a power surge, can also cause undesirable changes in data. Integrity refers to ensuring that data is accurate, full, trustworthy, and in its original form. Data that is missing or damaged can cause more harm than benefit.

Information integrity measures protect data from illegal alterations. These safeguards ensure that the data is accurate and trustworthy. Data kept in the system as well as data exchanged between systems, such as email, must be protected. It is not only required to limit access at the system level in order to maintain integrity, but also necessary to ensure that system users can only change information that they have been legally permitted to change.

Data integrity protection, like confidentiality protection, extends beyond the limits of vandalism. Accidental changes, such as human errors or data loss due to system failures, should also be prevented by effective integrity countermeasures. The financial industry must ensure that transactions on their systems are not manipulated with, even though all system owners must have confidence in the integrity of their data. In February 2016, cyber thieves fraudulently took $ 1 billion from the Central Bank of Bangladesh account at the Federal Reserve Bank of New York, in one of the most egregious recent breaches of financial data integrity. The hackers devised a well-thought-out strategy that included gaining the necessary credentials to make withdrawals, infecting the banking system with malware, destroying the transfer database records, and suppressing the confirmation messages to alert banking authorities to fraud. The majority of the transfers were halted or payments were recovered after the plan was detected, but the crooks were still able to make more than US $ 60 million. Integrity can be protected with a variety of countermeasures. Unauthorized users are prevented from making unauthorized access with access control and strong authentication. Hash checking and digital signatures can assist confirm that the transaction is genuine and that the file has not been tampered with. Management controls, such as division of roles and training, are just as critical as data integrity protection (Failed 2020).

Integrity refers to the capacity to assure that the system and its data have not been tampered with in any sense. Data is protected via integrity protection, but the operating system, applications, and hardware are also protected from illegal access. Cyclic Redundancy Check (CRC) is well recognized in automotive systems for providing integrity protection against non-malicious or inadvertent errors; nevertheless, it is not effective for preventing deliberate data alterations. As a result, sensitive data must include a cryptographic checksum for integrity verification. Furthermore, measures must be built to detect when data or system integrity has been compromised and to restore the impacted systems or data to their original state (Xu et al. 2011).

For example if anyone sends a parcel from one place to another. The parcel should be received by the receiver in the same form in which it is sent. In this way, integrity works with data. The data that is sent by the sender should be accurate, complete, and reliable. No alteration should be there while transmitting the data from source to destination.

Imagine what can happen if an organization transfers an employee's salary to an incorrect account owing to corruption of the database holding all employees' account number. This can impact badly on employees' account. This can happen because employee's database was not integrated.

The integrity relates two terminologies together which are as follows:

Data integrity: Assures that only specific and permitted changes are made to information and applications.

System integrity: Assures that a system performs its intended purpose without being harmed by intentional or unintentional unauthorized tampering (IEEE Approved Draft Guide for Engineering 2019).

Integrity refers to safeguarding against unauthorized information change or deletion, as well as ensuring non-repudiation and validity. The unlawful change or destruction of information is referred to as a loss of integrity.

Examples of allergy information from hospital patients kept in the database demonstrate the many features of completeness. The doctor must have confidence that the data is accurate and up-to-date. Assume that an employee with access to read and edit this information (for example, a nurse) purposefully falsifies data in order to ruin the hospital. The database must be rapidly restored to a stable state, and the error must be traced back to the person in authority. Information on a person's allergies is an example of a valuable asset that must be kept safe. Incorrect information can lead to significant fatality to the patient, putting the hospital underneath a lot of pressure (Sterpin et al. 2013).

A website that provides a forum for registered users to discuss particular topics, for example, may be labeled as an asset with a medium integrity criterion. Hackers or registered users can alter or destroy data on the website. The potential harm is minimal if the forum exists solely for the entertainment of its users, makes little to no advertising revenue, and is not used for critical purposes such as research. Webmasters may lose data, money, and time as a result of the attack. Anonymous Internet voting is an example of a system with low integrity requirements. Users can take these polls on many websites, including media organizations.

The following are some of the issues that could jeopardize the integrity of your data:

- Human error
- Compromising a system that lacks end-to-end encryption
- Physical device compromise

1.1.3 Availability

The availability of information is the third component of information security. The information that the organization creates and stores must be accessible to authorized parties. If the information is not readily available, it is pointless. Information must be updated on a regular basis, which necessitates that authorized parties have access to it. Information scarcity is just as destructive to a business as a lack of secrecy or integrity.

When a user enters data into a computer system, availability ensures that the data is available to the user when they require it. Users must have access to computer resources whenever they need them. It ensures that systems are up and running quickly and that authorized users are not refused service (Kang et al. 2014).

Consider the impact on a bank if consumers were unable to access their accounts for transactions. The more important the component or service, the higher the level of availability required.

Consider a system that enables essential systems, applications, and devices to be authenticated. Customers have been unable to access computer resources, and employees have been unable to access the resources required to execute key activities due to service outages. The loss of service translates into a significant economic loss in terms of employee productivity and possibly customer loss. The university's public website, for example, is frequently classified as a medium availability need because it gives information to existing and potential students as well as benefactors. Although such a site is not a critical component of the university's information system, its absence can be embarrassing. Low availability requirements will be assigned to online phone book search applications. Although losing an application for a short period of time can be inconvenient, there are other options for getting this information, such as printed catalog or operators.

In order for an information system to work, it must be accessible to authorized clients. Availability assessments ensure that users have access to the system at all times. Hardware failures, unplanned software downtime, and network bandwidth challenges are all examples of non-malicious threats to availability. Malicious attacks are a collection of several types of damage aimed at causing harm to an organization by denying clients access to the information system. Website availability and sensitivity are paramount for many companies. Even for short periods of time, disruption of website availability can lead to lost revenue, customer complaints, and reputation damage.

DoS (Distributed Denial of Service) attacks are a common way for hackers to interrupt web services. A DoS attack occurs when a hacker floods a server with unnecessary requests, overloading it and reducing service for legitimate users. Service providers have developed sophisticated defenses to identify and fight against DoS assaults over time, but hackers continue to evolve, and these attacks remain a threat. Only challenges to system availability have prompted widespread provisioning actions to protect system availability. Significant hardware redundancy and ready-to-use backup servers and data repositories are required for systems with high continuous uptime requirements. It is typical to have redundant systems in separate physical locations for large enterprise systems. Software tools for monitoring system performance and network traffic are required. Firewalls and routers are two methods for preventing DoS attacks (Islam and Sabrina 2009).

The higher the level of availability required, the more significant the component or service. Consider a system that enables essential systems, applications, and devices to be authenticated. Customers have been unable to access computer resources, and employees have been unable to access the resources required to execute key activities due to service outages. The loss of service translates into a significant economic loss in terms of employee productivity and possibly customer loss.

1.1.4 Non-repudiation

To repudiate means to deny or contest something. Therefore, non-repudiation must be the ability to ensure that someone cannot deny or contest that thing. This is usually seen in electronic communications where one side denies seeing or signing a contract or paper or cannot be confirmed as the recipient. Non-repudiation means putting measures in place that will prevent one party from denying they received or agreed to a transaction.

1.2 Access Control

Authentication and authorization are the keys to access control. In terms of security, access management is vital (Bauer et al. 2005).

Access Control

It is "the process of approving or rejecting various requests." The following components are considered for this procedure:

- Who was the one who made the request?
- What is being asked for?
- Which rules apply when making a decision on the request?

To begin, the source of a request may be a specific computer, a machine in a specific configuration, or a specific application, such as an Android app.

Second, on a technological level, requests in a machine are issued by a process rather than a human. "For whom or for what is the method speaking while requesting?" the query is transformed into the phrase "what is asked" generally refers to a combination of an action to be performed and the object on which the action will be performed. This is accomplished through the usage of rules. Rules are logical formulations that are evaluated to provide a result. Allow or refuse is the choice.

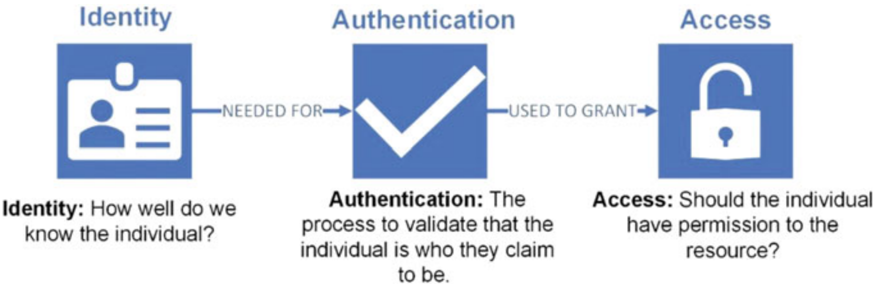

Identity
Authentication
Access
NEEDED FOR
USED TO GRANT
Identity: How well do we know the individual?
Authentication: The process to validate that the individual is who they claim to be.
Access: Should the individual have permission to the resource?

Fig. 1.2 Relationship between identity, authentication, and access

Access Control (ISO/IEC 27,000, 2009) refers to the process of allowing and controlling access to assets based on business and security requirements. The practice of monitoring and regulating who has access to what systems, information, or data is known as access control. In almost all the cases, access must be restricted to people or computers who have been given authorization. To manage access based on rights, it generally follows the phases of identification, authentication, and authorization. By providing a log, for example, a better accountability method can achieve an entity's responsibility for its activities (Foley et al. 2011).

1.2.1 Identification

The procedure is recognizing or acknowledging a person or system. An identity will be checked during the identification procedure, which may or may not be true. A public piece of information, such as a username or an identification number, is usually provided by the subject (see Fig. 1.2).

1.2.2 Authentication

Authentication is the process of verifying that a user's identity is genuine. Most systems require a user to be authenticated prior to granting access to the system (Saxena et al. 2014). The user does this by entering a password, inserting a smart card, and entering the associated personal identification number (PIN), providing a biometric (e.g., fingerprint, voice pattern sample, retinal scan)—or a combination of these things—to prove they are who they claim to be. The credentials provided are compared to those that have previously been associated with the user. The credential match may be performed within the system being accessed or via a trusted external source. If the credentials match, the system authenticates the identity and grants access (see Fig. 1.2).

Authentication is defined by the International Organization for Standardization (ISO) as "providing assurance that a claimed attribute of an object is actual" (ISO/IEC 27,000, 2009).

In information security, a user is often identified by a username (public) and a password (private information). The username will be used to claim an identity, and the password will be compared to a previously saved user password to confirm the user's identity. The user is authenticated if the username and password match.

Biometric information, such as a fingerprint, or electrical technology, such as RFID tokens or smart cards, can also be used for identification and authentication. Different identifying approaches differ in terms of effort, dependability, and security. A combination of measures (multifactor authentication) may improve security and lower the danger of identity theft; for example, if an RFID tag is used to identify a person, the risk of identity theft is reduced.

The three general features (i.e., components) utilized to authenticate identification are as follows (Yuan et al. 2002).

1. Something the user owns or possesses (for example, a token or smart card)
2. Something the customer recognizes (a phrase or a PIN)
3. Something to which the user alone has access (e.g., biometric identification) (Crowe et al. 2004).

1.2.3 Authorization

It is the process of determining and approving authorized users' access permissions. It also describes what data and actions a properly identified and authenticated person or machine is permitted to access and perform.

1.2.3.1 Access Control Models

Access control models, which govern how individuals can access things, enforce the rules and goals of a given security policy. Here is a quick rundown of the three most common access control models.

1. **Discretionary Access Control (DAC)**: This model allows the owner or the creator who has created the item, such as a file, to control who has access to it and who does not. As a result, identity-based access control is another name for DAC (IBAC) (Li 2008).
2. **Mandatory Access Control (MAC)**: Categories are used in Mandatory Access Control (MAC) to identify what the subject (user) needs to know. When a person's clearance level is higher than or equal to the classification of an item, he or she has access to all of it (data or information). It is also known as a rule-based access control system (Zou et al. 2009).

3. **Role-Based Access Control (RBAC)**: The most generally used paradigm distributes permissions to a subject based on roles or groups. The resources that his or her group(s) or role(s) have access to will be available to the user. For example, an administrator might create a group for a job title or department-related rights and assign the appropriate personnel to it. As a result of this creation of group, administrative labor is decreased (Saxena et al. 2017).

1.2.3.2 Techniques of Access Control

The access control matrix is a system for linking a subject's access permissions to a specific item. It is one of the most commonly used mechanisms for access control. The rows reflect the user's capability table, while the columns represent the resource's Access Control List (ACL). The access rights and privileges that a user has resources on a system, such as files and directories, are identified using an Access Control List.

The following privileges are typical in an operating system and file system environment (Gattiker 2004):

- Read—to read a file or a directory's contents
- Write—to create or edit files/directories
- Execute—this command is used to run a file, such as a program.

1.2.3.3 Implementation of AAA

AAA establishes a uniform framework for managing who has access to a router, what services they can access, and what they can do with it. The sections below discuss the functions of AAA as well as how to activate it. AAA Functions AAA includes three basic components: authentication, authorization, and accounting.

AAA's authentication: This component is responsible for allowing users to be recognized (authenticated). Login access is an example, as are other types of access, such as PPP network access. When a user uses AAA authentication, you specify one or more authentication methods that the router should employ. You might, for example, provide two authentication methods: use an external security server if one is available and utilize the router's local username database if one is not (refer Fig. 1.3).

AAA's authorization: It is the process of implementing regulations by establishing what types of activities, resources, or services a user is permitted to engage in.

AAA's accounting: Accounting is the final component of the AAA architecture, and it keeps track of how much bandwidth a user uses while on the network. The amount of system time or the amount of data delivered and received during a session are examples of this. Accounting is done by keeping track of session statistics and consumption data.

AAA implementation: AAA may be implemented utilizing either the device's internal database or an external ACS (Access Control server) (Decugis 2009).

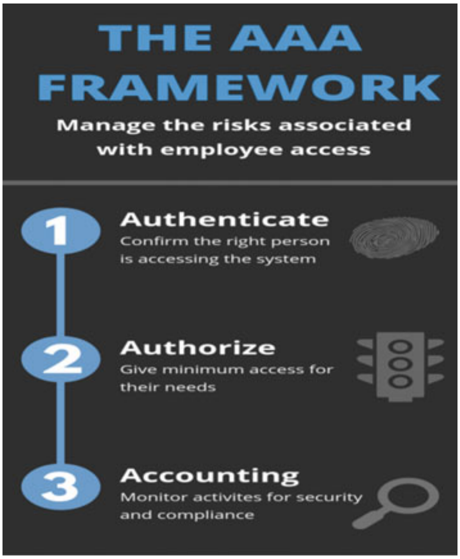

THE AAA FRAMEWORK
Manage the risks associated with employee access
1
Authenticate
Confirm the right person is accessing the system
2
Authorize
Give minimum access for their needs
3
Accounting
Monitor activites for security and compliance

Fig. 1.3 AAA framework

- **Local database**—To implement AAA using the router or switch's local operational configuration, we must first create users for authentication and then give permission levels to those users for authorization.
- **ACS server**—This is the most often used technique. An external ACS server is utilized for both the router and the ACS must be configured, and AAA (which could be ACS hardware or software installed on VMware (Free Virtualization for Windows and Linux Servers)). The setup includes creating a user and a unique customization method list for authentication, authorization, and accounting.

The client or Network Access Server (NAS) makes an authentication request to the ACS server, which decides whether or not to provide the user access to the network resource based on the credentials given by the user.

The concept of virtualization has brought major changes on the concepts of authentication, authorization and accounting part of the business.

Important: If the ACS server fails to authenticate, the administrator should specify that the device's local database will be utilized as a backup in the method list.

AAA in Devices made by CISCO

There are two common methods defined by Cisco for implementing AAA services:

- **Local AAA Authentication**—For authentication, local AAA uses a local database. Self-contained authentication is the name given to this approach. It will be referred to as local AAA authentication in this course. Users authenticate against a local database in the Cisco router, which stores users and passwords. This is the same database that is required to set up the role-based CLI.

- **Server-Based AAA Authentication**—A server-based approach, such as the Cisco Secure Access Control System (ACS) for Windows, links the router to a central AAA server. All users' usernames and passwords are stored on the central AAA server. The router uses either the Remote Authentication Dial-In User Service (RADIUS) or the Terminal Access Controller Access Control System (TACACS+) protocol to connect to the PC with the AAA server. Server-based AAA is more suited when there are many routers and switches.

Once a user has been authorized, a session is established between the router and the AAA server.

The router requests authorization for the client's requested service from the AAA server.

Access Control Server (ACS) is used to provide a centralized administration system for the authentication, authorization, and accounting (AAA framework).

TACACS and RADIUS are the protocols used to communicate between the client and the ACS server.

1.2.4 Accountability

When someone logs into a network and begins working, their activities should be tracked. This can be assisted by a SIEM (Security Information and Event Management) or other auditing and monitoring technology. Knowing what files someone is looking at or attempting to access can assist establish whether more or less authorization is needed. Suspicious behavior may raise questions about whether the individual is trustworthy.

For this reason, all important system activities, events, and processes, such as failed and successful authentication attempts, are logged. An audit trail, also known as an information audit, is a chronological record of system operations that can be used to reconstruct and analyzes the actions of a system.

There are many different forms of network assaults, such as loop attacks, chain attacks, and doorknob attacks. The accountability algorithms may be used in conjunction with distributed recognition to provide robust responsibility for every individual network movements. For accountability, the DRA algorithm can be employed.

1.3 Cryptography

- **plaintext**—the message as it was originally sent
- **ciphertext**—a message that has been coded
- **cipher**—algorithm for converting plaintext to ciphertext
- **key**—information used in cipher that is only known by the sender/receiver
- **encipher (encrypt)**—converting plaintext to ciphertext

- **decode (decrypt)**—retrieving ciphertext from plaintext cryptography
- **Cryptanalysis (code breaking)—**study of the concepts and methods for decoding ciphertext without the knowledge of the key.
- **Cryptology**—Cryptography and cryptanalysis are both included in this field.
- Anyone who needs to verify the CA's statement of public-key ownership can utilize the public key.

Digital certificates, in contrast, still require a chain of trust to ensure that the certificate belongs to the person or organization you believe in and that it has not been tampered with. Criminals are accused of obtaining certificates and then using them to sign malware-infected software. Malicious software was detected.

Cryptography

The rapid advancement of cutting-edge Internet technology and data innovation has led to an increase in the number of individuals, businesses, and government offices joining the Internet. Which has resulted in an increase in the number of criminals attacking businesses by using fictitious websites and sending counterfeit messages? The focus of the assaults and interruptions on the organization is PCs, so if the gatecrashers succeed, a large number of organization PCs will be rendered inoperable. Additionally, a few trespassers with ulterior thought processes see the military and government division as the goal, posing enormous risks to social and public safety (Latif et al. 2020; Ahmad et al. 2009). Cryptography denotes "Covered up Secrets" is concerned with encryption. Cryptography is the study of frameworks for secure communication. It can be used to examine shows that are related to numerous aspects of information security, such as check, data grouping, non-disavowal, and data uprightness.

The study of writing secret codes is called cryptography. It is primarily concerned with the design and exploration of conventions that hinder opponents. Different views on data security, such as information confidentiality, information reliability, validation and non-repudiation, are very important for encryption today.

Two terms are of decisive importance in cryptographic calculation, they are as follows:

1. *Unconditional Security*

Regardless of the computing power or time available, the code cannot be decrypted because the ciphertext does not contain enough information to clearly identify the plain text.

2. *Computational Security*

The encryption cannot be broken due to inadequate computational resources (for example, the time required for calculations are larger than the age of the universe) (Sasubilli et al. 2020).

Cryptographic framework can be portraying by:

1. Type of encryption activities used:

That can be substitution or rendering of item.

2. Number of keys used

That can be single-key or private/two-key or public.

3. Way of plain text handling

The way plain text is either block or in the form of stream.

1.3.1 Symmetric Encryption

Symmetric and unbalanced encryption strategies are the most common approaches used to encode/ decrypt protected data. When symmetric encryption is required, the same cryptographic keys are used for text encryption and decryption of image content. Although symmetric-key encryption is faster and easier to use, it has the disadvantage of requiring both parties to relocate their shared key (Bani Baker and Al-Hamami 2017) refer Fig. 1.4.

To use symmetric encryption safely, there are two requirements:

- a robust and computationally infeasible encryption algorithm
- a secret key that is only known by the sender and receiver parties

Mathematically we have:

$$Y = E_K(X)$$
$$X = D_K(Y)$$

It assumes that encryption algorithm is known and implies a secure path to distribute key.

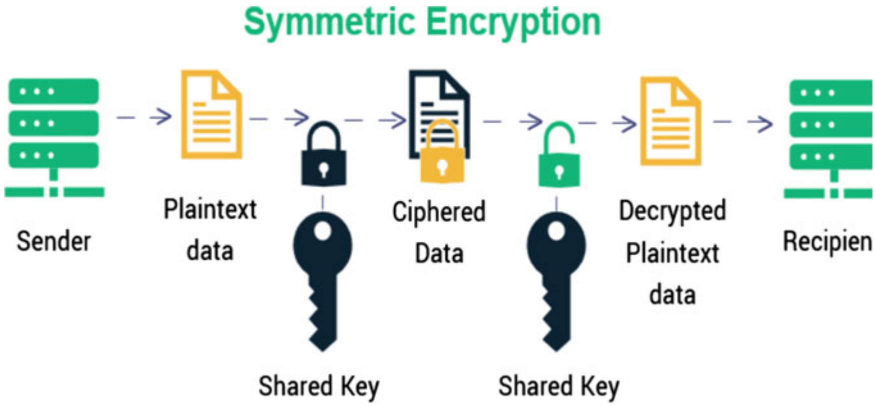


Fig. 1.4 Symmetric encryption

Types of symmetric-key algorithms Symmetric-key encryption:

1 **Classical Substitution Ciphers**

Plaintext letters are substituted with other letters, numbers, or symbols in this method. The well-known schemes under classical ciphers are Caesar Ciphers, Mono alphabetic Ciphers, Playfair Ciphers, Poly alphabetic Ciphers, Vigenère Cipher, Kasiski Method, Auto key Cipher, and One Time Pad (Failed 2014).

2 **Transposition Ciphers**

These methods hide the information by rearranging the order of the letters without changing the letters actually used; however, they are recognizable because they have the same frequency distribution as the original text. Types are Rail Fence cipher, Row Transposition Ciphers, Product Ciphers, Rotor Machines, and Hagelin Rotor Machine.

1.3.2 Asymmetric Encryption/Private Key Cryptography

Asymmetric encryption, commonly known as public-key cryptography, uses two keys. The two keys are a public key that is accessible to the general public and a private key that is only accessible to the user.

Message data is encrypted using a recipient's public key in public-key encryption. Anyone who does not have the coordinating private key will not be able to see the message. This is a privacy strategy (Failed 2014) (Fig. 1.5).

Public key was created to address two major concerns.

The *first* is key distribution, or how to establish secure communications without entrusting your key to a key distribution center (KDC). It does not require secure key distribution, and it does not require anyone else to know your private key.

Another concern is digital signatures, which are electronic stamps that ensure a communication is sent by the specified sender. In electronic stamps, a message is endorsed with the sender's private key, which can be reviewed by anybody who has access to the private key, ensuring the organization's security (Saxena et al. 2014).

Calculations based on public keys are based on two keys that have the following characteristics:

- It is computationally impossible to figure out the decoding key using only the calculation and encryption keys.

When the important (scramble/unscramble) key is known, it is computationally straightforward to encode/decode messages.

- For encryption, one of the two related keys can be used, while the other can be used for decoding (in certain plans) (Figs. 1.6, 1.7, 1.8)
- **Public-Key Cryptosystems showing Secrecy**

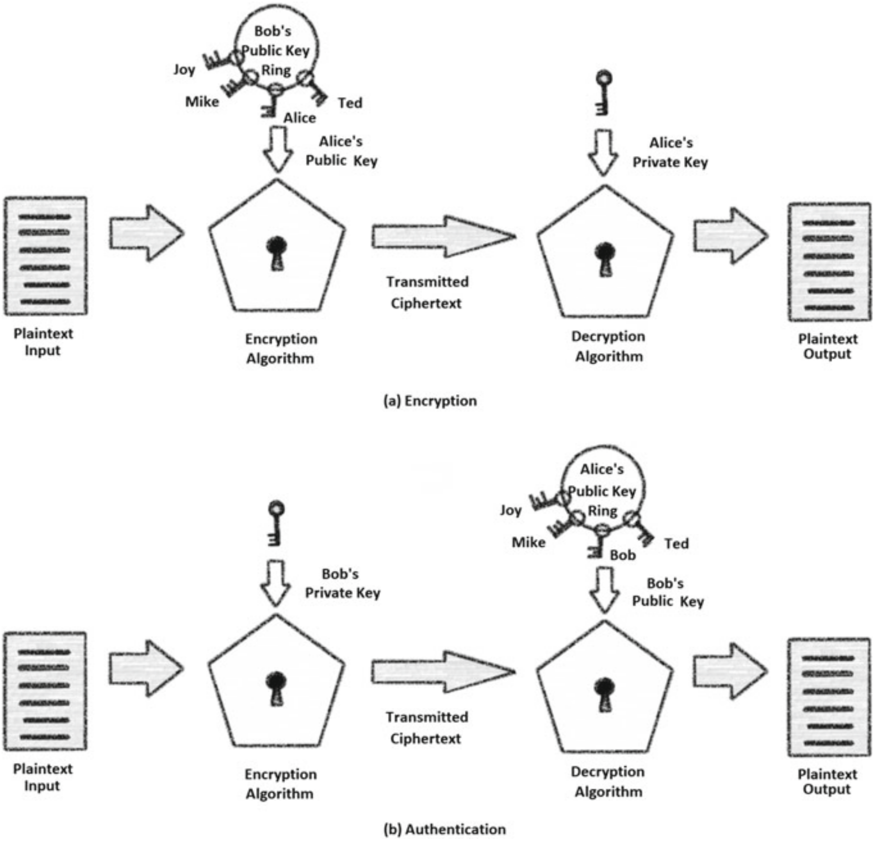


Fig. 1.5 **a** Encryption. **b** Authentication

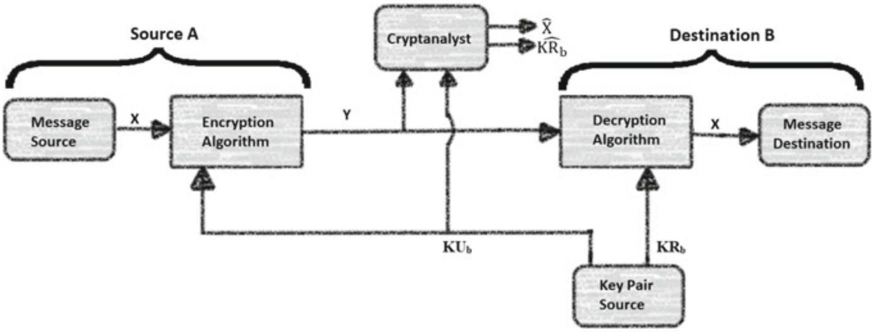


Fig. 1.6 Public-key cryptosystem showing secrecy

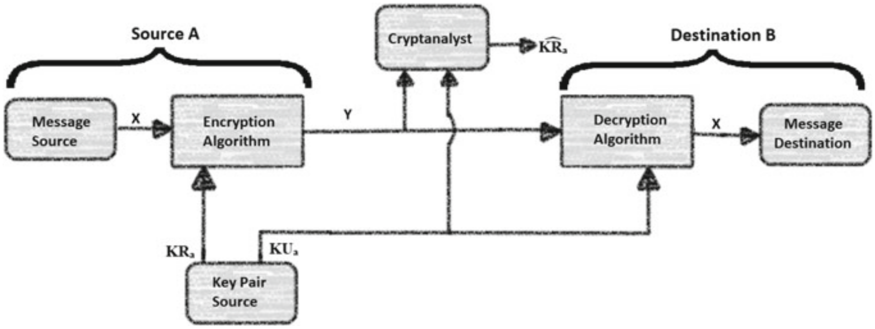


Fig. 1.7 Public-key cryptosystem showing authentication

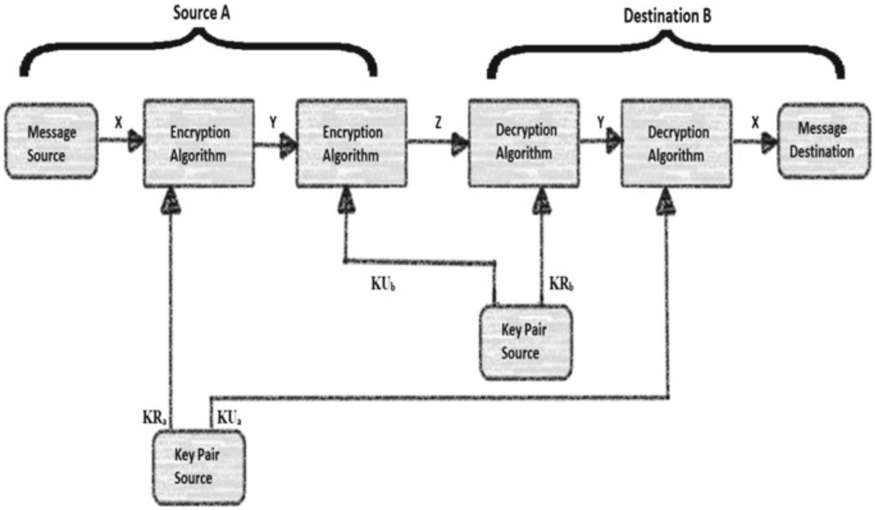


Fig. 1.8 Public-key cryptosystem showing secrecy and authentication

- **Public-Key Cryptosystems showing authentication**
- **Public-Key Cryptosystems showing Secrecy and Authentication**

An open key cryptosystem must meet following conditions:

1. With the appropriate key, encoding or translating a message is simple.
2. Inferring the private key from the open key is impossible.
3. Making a decision on the private key from a selected plaintext attack is impossible.

For the most part, these conditions ensure that scrambled data can be decoded with the appropriate private key. In today's world, three open key calculations are routinely used.

Diffie–Hellmann (DH), named for its distributors Whitfield Diffie and Martin Hellman in 1976, could also be a key-trading convention, for example, to securely exchange passwords via an open or shared medium, similar to the web. The Computerized Signature Calculation (DSA) is used for computerized marks, despite the fact that RSA15 is appropriate for advanced marks and encryption.

Public-Key Applications: They can classify into 3 categories:

- encryption/decryption (provide secrecy)
- digital signatures (provide authentication)
- key exchange (of session keys)

Some algorithms are suitable for all uses, others are specific to one.

RSA Algorithm:

RSA by Rivest, Shamir & Adleman of MIT in 1977, best known and widely used public-key methods based on exponentiation of integers in a finite field. The **RSA Algorithm** is an asymmetric cryptography algorithm; this means that it uses a *public* key and a *private* key (i.e., two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone (Radhakrishnan and Akila 2021).

RSA Key setup

Each user generates a public/private key pair by:

1. Select two large prime numbers, x and y. The prime numbers need to be large so that they will be difficult for someone to figure out.
2. Calculate $n = x\ x\ y$.
3. Calculate the totient function; $\phi(n) = (x - 1)(y - 1)$.
4. Select an integer e, such that e is co-prime to $\phi(n)$ and $1 < e < \phi(n)$. The pair of numbers (n, e) makes up the public key.
5. Calculate d such that $e.\ d = 1 \bmod \phi(n)$.

d can be found using the extended Euclidean algorithm. The pair (n, d) makes up the private key.

Encryption

Given a plaintext P, represented as a number, the ciphertext C is calculated as:

$C = \mathrm{Pe} \bmod n$

Decryption

Using the private key (n, d), the plaintext can be found using:

$P = d \bmod n.$

RSA Example

1. Select primes: $p = 17$ and $q = 11$
2. Compute $n = pq = 17 \times 11 = 187$
3. Compute $\varnothing(n) = (p - 1)(q - 1) = 16 \times 10 = 160$
4. Select e: $\gcd(e, 160) = 1$; pick $e = 7$
5. Determine d: $\mathrm{de} = 1 \bmod 160$ and $\mathrm{d} < 160$ Value is $d = 23$

Since $23 \times 7 = 161 = 10 \times 160 + 1$

6. Publish public-key KU = {7,187}
7. Keep mystery private key KR = {23, 17, 11}
8. Sample RSA encryption/decoding is:
9. Given message $M = 88$ $(88 < 187)$
10. Encryption:
11. $C = 887 \bmod 187 = 11$
12. Decryption
13. $M = 1123 \bmod 187 = 88$.

References

Ahmad A, Biri A, Afifi H, Zeghlache D (2009) TIBC: trade-off between identity-based and certificateless cryptography for future internet. In: 2009 IEEE 20th international symposium on personal, indoor and mobile radio communications, pp 2866–2870. https://doi.org/10.1109/PIMRC.2009.5450118

Al-Mohammed HA, Al-Ali MS, Alkaeed M (2020) Quantum computer architecture from non-conventional physical simulation up to encryption cracking. Machine learning application, and more. In: 2020 16th International Computer Engineering Conference (ICENCO), pp 17–24. https://doi.org/10.1109/ICENCO49778.2020.9357401

Bani Baker SI, Al-Hamami AH (2017) Novel algorithm in symmetric encryption (NASE): based on Feistel cipher. In: 2017 international conference on new trends in computing sciences (ICTCS), pp 191–196. https://doi.org/10.1109/ICTCS.2017.54

Bauer L, Garriss S, Reiter MK (2005) Distributed proving in access-control systems. In: 2005 IEEE symposium on security and privacy (S&P'05), pp 81–95. https://doi.org/10.1109/SP.2005.9

Biswas C, Gupta UD, Haque MM (2019) An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography. In: 2019 international conference on electrical, computer and communication engineering (ECCE), pp 1–5. https://doi.org/10.1109/ECACE.2019.8679136

Bhowal S, Dutta SR, Mitra S (2017) An efficient reduced set brute force attack technique for a particular steganographic tool using vername algorithm. Fourth Int Conf Image Inform Process (ICIIP) 2017:1–4. https://doi.org/10.1109/ICIIP.2017.8313698

Crowe TW, Bishop WL, Porterfield DW, Hesler JL (2004) Integrated terahertz sources and receivers. In: Infrared and Millimeter waves, conference digest of the 2004 joint 29th international conference on 2004 and 12th international conference on terahertz electronics, 2004, pp 85–86. https://doi.org/10.1109/ICIMW.2004.1421965

Decugis S (2009) Towards a global AAA framework for internet. Ninth Ann Int Symp Appl Internet 2009:227–230. https://doi.org/10.1109/SAINT.2009.57

Foley SN, Fitzgerald WM, Adams WM (2011) Federated autonomic network access control. In: 2011 4th symposium on configuration analytics and automation (SAFECONFIG), pp 1–2. https://doi.org/10.1109/SafeConfig.2011.6111668

Gattiker A (2004) Diagnosis meets physical failure analysis: how long can we succeed? In: 2004 international conference on test, p 1441. https://doi.org/10.1109/TEST.2004.1387449

Hambouz A, Shaheen Y, Manna A, Al-Fayoumi M, Tedmori S (2019) Achieving data integrity and confidentiality using image steganography and hashing techniques. In: 2019 2nd international conference on new trends in computing sciences (ICTCS), pp 1–6. https://doi.org/10.1109/ICTCS.2019.8923060

https://www.includehelp.com/cryptography/introduction.aspx

IEEE PC37.250/D1.30 (2019) IEEE approved draft guide for engineering, implementation, and management of system integrity protection schemes, pp 1–68, 5 March 2020

Islam ABMAA, Sabrina T (2009) Detection of various denial of service and Distributed Denial of Service attacks using RNN ensemble. In: 2009 12th international conference on computers and information technology, pp 603–608. https://doi.org/10.1109/ICCIT.2009.5407308

Kang S, Veeravalli B, Mi Aung KM, Jin C (2014) An efficient scheme to ensure data availability for a cloud service provider. In: 2014 IEEE international conference on big data (Big Data), pp 15–20. https://doi.org/10.1109/BigData.2014.7004378

Latif MA, Ahmad MB, Khan MK (2020) A review on key management and lightweight cryptography for IoT. Global Conf Wirel Opt Technol (GCWOT) 2020:1–7. https://doi.org/10.1109/GCWOT49901.2020.9391613

Li N (2008) How to make discretionary access control secure against trojan horses. IEEE Int Symp Parall Distrib Process 2008:1–3. https://doi.org/10.1109/IPDPS.2008.4536104

Ma D, Wang L, Lei C, Xu Z, Zhang H, Li M (2016) Thwart eavesdropping attacks on network communication based on moving target defense. In: 2016 IEEE 35th international performance computing and communications conference (IPCCC), pp 1–2. https://doi.org/10.1109/PCCC.2016.7820610

Mandal B, Chandra S, Alam SS, Patra SS (2014) A comparative and analytical study on symmetric key cryptography. In: 2014 international conference on electronics, communication and computational engineering (ICECCE), pp 131–136. https://doi.org/10.1109/ICECCE.2014.7086646

Martin T (2011) Undecryptable symmetric encryption. IEEE GCC Conf Exhib (GCC) 2011:225–228. https://doi.org/10.1109/IEEEGCC.2011.5752504

Radhakrishnan S, Akila A (2021) Securing distributed database using elongated RSA algorithm. In: 2021 7th international conference on advanced computing and communication systems (ICACCS), pp 1931–1936. https://doi.org/10.1109/ICACCS51430.2021.944196

Sala O et al (2021) SafeTI: a hardware traffic injector for MPSoC functional and timing validation. In: 2021 IEEE 27th international symposium on on-line testing and robust system design (IOLTS), pp 1–7. https://doi.org/10.1109/IOLTS52814.2021.9486689

Sasubilli SM, Dubey AK, Kumar A (2020) A computational and analytical approach for cloud computing security with user data management. Int Conf Adv Comput Commun Eng (ICACCE) 2020:1–5. https://doi.org/10.1109/ICACCE49060.2020.9154975

Saxena S, Sanyal G, Srivastava S et al (2017) Preventing from cross-VM side-channel attack using new replacement method. Wireless Pers Commun 97:4827–4854

Saxena S, Sanyal G, Srivastava S (2014) Mutual authentication protocol using identity-based shared secret key in cloud environments. In: International conference on recent advances and innovations in engineering (ICRAIE-2014), pp 1–6. https://doi.org/10.1109/ICRAIE.2014.6909267

Sterpin I, Kirincic V, Skok S (2013) The educational model of the system integrity protection scheme. In: 2013 36th international convention on information and communication technology, electronics and microelectronics (MIPRO), pp 1235–1240

Tugnait JK (2016) Detection of active eavesdropping attack by spoofing relay in multiple antenna systems. IEEE Wirel Commun Lett 5(5):460–463. https://doi.org/10.1109/LWC.2016.2585549

Wu Y, Zhang X, Li W (2020) Research on data integrity protection technology of industrial control network. In: 2020 5th international conference on mechanical, control and computer engineering (ICMCCE), pp 755–758. https://doi.org/10.1109/ICMCCE51767.2020.00166

Xu Z, Wen A, Liu Z (2011) Some transforms in cyclic redundancy check (CRC) computation. Int Conf Electr Control Eng 2011:3154–3156. https://doi.org/10.1109/ICECENG.2011.6057364

Yuan S et al (2002) Advanced write heads for high density and high data rate recording. In: 2002 IEEE international magnetics conference (INTERMAG), pp BA5. https://doi.org/10.1109/INTMAG.2002.1000774

Zou D, Shi L, Jin H (2009) DVM-MAC: a mandatory access control system in distributed virtual computing environment. In: 2009 15th international conference on parallel and distributed systems, pp 556–563. https://doi.org/10.1109/ICPADS.2009.128

Chapter 2
Basic Concepts of Cloud and Fog Computing

Sahil Kansal

2.1 Cloud Computing and Its Applications

Cloud computing itself is not standalone computing model. It is evolved through different computing models. This section presents the evolution of cloud computing and definition of cloud computing.

2.1.1 Evolution of Cloud Computing

Cloud computing is the evolution of the distributing computing. Different distributed computing models came into existence one after the other as per the requirement. Cluster computing, grid computing, utility computing, and then cloud computing, this is how different computing models have evolved. Brief description of these models is giving as below (NIST 2011; Saxena et al. 2015):

Cluster Computing: In the cluster computing, multiple computers are connected together for the execution of the single task. The increasing demand of the user's jobs has brought the emergence of cluster computing. These systems are connected through high-speed local area network to prevent the high latency and serves as the single entity. The clusters are tightly coupled where same operating system and hardware are used at the same physical location. The clusters are managed centrally by the resources manager and provide limited capacity, robustness, and limited privacy.

Grid Computing: In grid computing, multiple resources/computers from different administrative domain are combined together for the execution of the single user's

S. Kansal (✉)
Galgotias College of Engineering and Technology, Greater Noida, India
e-mail: sahil.kansal@galgotiacollege.edu

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_2

task. Systems in the grid computing are loosely coupled and can operate in combination with different operating systems installed over them and different systems' configurations. The systems are connected through Internet at multiple physical locations and cause high latency. In the grid computing, the user's task is distributed amongst the multiple systems for the parallel execution of the task.

Utility Computing: This computing model is similar to the cloud computing and requires cloud computing resources. The resources are provided to the users on-demand basis. The main advantage of the utility computing is that users do not require purchasing the infrastructure resources; the resources are available from the third party. But, due to its limiting characteristics like privacy, reliability, and security, utility computing has lost its sustainability in the market.

Cloud Computing: Cloud computing holds very important position. Cloud computing is the extension of the utility computing. In this computing model, resources are provided as services to the users on-demand basis. The cloud services are metered; the users have to pay only for the services being used. The services are scalable and flexible. Users can extend the service requirements dynamically and automatically without and human intervention. Once the resources utilized, it can be released back to the provider. Cloud computing provides very economical way of delivering the IT resources and proved to be a boon for small IT companies. Cloud computing has made the companies to work on the business logic without bothering about the operational and computational aspects of the of IT resources.

The above distributed computing models show the evolution of cloud computing model. But, if we see how evolution has taken place years after year, and decade after decades, the very clear evolution is shown below (Saxena et al. 2015):

1950	Time Shared Mainframe Computer
1969	ARPANET
1970	Virtual Machines by IBM
1990	Inception of VPN
1996–97	Cloud Computing
1999	Sales force.com
2002	AWS
2006	Amazon Ec2
2008	Google App Engine/ Microsoft Azure

2.1.2 Definition of Cloud Computing

Cloud computing is the computing service model that allows the provisioning of the information technology (IT) resources, *i.e.* computing power, storage, physical memory, bandwidth, etc., as services to the end users. It is the evolution of the existing distributed computing paradigms like grid and utility computing. It has been termed as the fifth utility after electricity, gas, water, and telephony because like these utilities, cloud provides the basic computing resources on demand to the cloud users and charge the consumers only for the amount of resources being used (Buyya et al. 2009). Cloud computing has shifted the way the organization look at the IT resources (Srivastava et al. 2021). It had made the possibility of provisioning of the resources at very low cost and has freed the consumers (individuals and small organizations) form the purchasing and maintaining in-house IT resources, consequently allowing organizations to focus on the business operations only. It had opened the gates for small organization to grow as it empowered them to extend their resource requirements at very low cost (Gupta et al. 2013). Nearly half of the company's expenses spend in purchasing, maintaining, and supporting the IT resources only. So, for the organizations that could not afford the high requirement of IT resources, cloud computing has emerged as the most valuable asset. Even the scientific applications that require the very high-computation resources for small duration only can utilize the cloud resources on pay as use basis.

The features of cloud computing are so different that it cannot be explained in single definition. It has been defined differently by the many researchers. National Institute of Standard and Technologies (NIST) has defined cloud computing as follows (NIST 2011):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

2.1.3 Essential Characteristics of Cloud Computing

Cloud computing holds the multiple aspects of grid and utility computing (Galante et al. 2016), virtualization, and automatic computing (Kavis 2014). Its significant features distinguished it from the other existing distributed computing models and made it widely accepted by the users and organizations globally. All these characteristics are described as follows (Rappa 2004; Zhang et al. 2010; Foster et al. 2008):

(1) *Utility driven pricing*: Cloud computing offers the services in pay as use manner. Resources are allocated dynamically to the consumers and de-allocated whenever not required. The consumers have to pay only for the amount of resources and for the duration, when resources are being consumed. For example, the scientist wants to run the application that requires high-computation power for the small duration of time. For this purpose, consumers have to pay for the computation power for that duration of time only.

(2) *Shared resources (multi-tenancy)*: In cloud computing, the pool of interconnected resources is allocated in the form of virtual machines (VMs). The virtualization allows the sharing of underlying hardware by the multiple VMs,

thereby making efficient utilization of the resource. Each VM acts as an independent operating system platform for different user's request and can dynamically reconfigured according to the user's request. One of the key advantages of the VM is that it allows the dynamic allocation and de-allocation of the resources and provides the migration of the VMs from one data centre to another.

(3) *Dynamic resource provisioning*: The resources in the cloud computing are dynamically and elastically provided by the service providers. The user can extend the requirement for resources on the fly and can release the resources whenever required. This dynamic behaviour of cloud computing is mainly advocated by the virtualization. In cloud, the resources are primarily delivered in the form of VMs. These VMs are created when demanded by the consumers and terminated after the completion of the specific task.

(4) *Self organizing*: In cloud computing, all the processes of resource allocating and de-allocating are carried out automatically without human intervention. All the mechanisms like scheduling, virtual machine migration, server consolidation, and resource management are mechanized.

(5) *Resilient*: The data on the cloud are replicated to the multiple data centres at different geographic locations. This provides the seamless functioning of the cloud services, thereby providing the robustness and fault tolerance to the cloud data.

2.1.4 Cloud Computing: Layered Architecture

Cloud computing offers different types of services that vary from underlying IT resource to the application services. These services have been broadly divided the cloud computing environment into four layered architectures as shown in Fig. 2.1. The layers are data centre, infrastructure, platform, and application. Each layer operates differently as explained below.

(1) *Data centre layer*: This layer consists of the underlying physical resources like physical servers, switches, routers, cooling, and systems. This layer is the network of multiple servers and is responsible for the management of the physical resource on the cloud computing.

(2) *Infrastructure layer*: This layer provides the infrastructure-as-a-service (IaaS) and is responsible for the sharing of the resource at the data centre layer. It is also known as the virtualization layer as all the multiple combination of the storage, memory, computing power, and bandwidth in the form of VMs is provided by the infrastructure layer. The layer regulates the allocation of the resources to the user's request using the virtualization technologies like KVM, Oracle virtual box, VMware, etc.

(3) *Platform layer*: This layer on the top of infrastructure layer provides preconfigured VMs and required platform, for the development and the execution of certain technology (*i.e.* Java, .Net, etc.)-based applications. The main

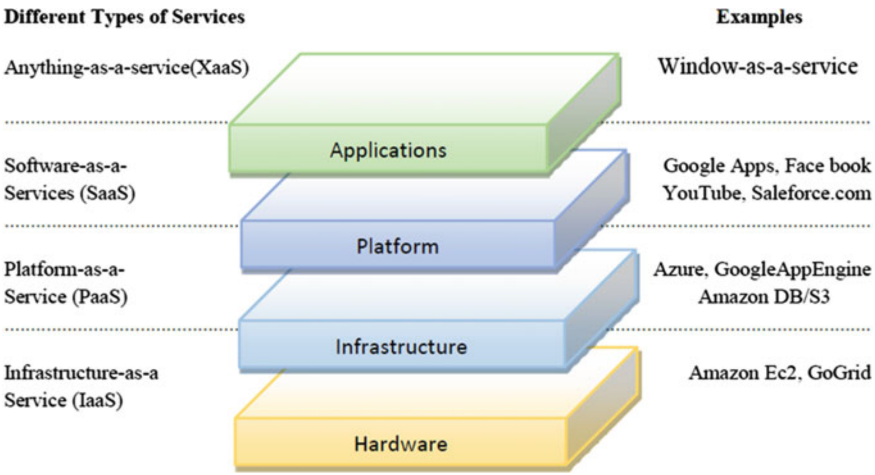

Different Types of Services
Examples
Anything-as-a-service(XaaS)
Window-as-a-service
Applications
Software-as-a-Services (SaaS)
Google Apps, Face book YouTube, Saleforce.com
Platform
Platform-as-a-Service (PaaS)
Azure, GoogleAppEngine Amazon DB/S3
Infrastructure
Infrastructure-as-a Service (IaaS)
Amazon Ec2, GoGrid
Hardware

Fig. 2.1 Cloud computing layered services (Zhang et al. 2010)

purpose of this layer is to reduce the burden of installing the platform on the VM by the user. For example, Google App engine provides the working environment for the Java and Python-based application.

(4) *Application layer*: Lies on the top of all layers, application layer provides pre-installed application like Microsoft office 365, sales force, etc., that allows the consumers to directly use the applications for specific purpose.

All these layers are loosely coupled and allow each other to operate individually to provide specific services. Based on the different type of services, Fig. 2.1 shows the cloud services that have been classified as

(a) *Infrastructure-as-a-service (IaaS)*: In IaaS, the infrastructure resource like storage, memory, processing power, and bandwidth are provided as services to the user, and these resources are provisioned in the form of VMs. The user can install and manage operating system and applications over them but does not have control over the underlying infrastructure. For example, Amazon Web Services (AWS), Microsoft azure, Google Compute Engine, etc.

(b) *Platform-as-a-service (PaaS)*: These services provide the platform for the development and execution of the application pertaining to specific technology. In PaaS, consumers are given pre-installed platform using VM container, and users just have to develop and run the applications. For example, Google App Engine, Apache Stratos, Window Azure, etc.

(c) *Software-as-a-service (SaaS)*: In SaaS, the consumer is given access to the application like Microsoft Office. The user can use the functions of that application and can manage files but does not had control over operating system and underlying hardware. For example, Google docs, Microsoft Office 365, etc.

(d) *XaaS (Anything-as-a-service)*: NIST has defined the different cloud service types as SaaS, PaaS, and IaaS. But currently vendors are coming up with the new and numerous ways of delivering services using cloud that may include database-as-a-service (DBaaS), window-as-a-service (WaaS), malware-as-a-service (MaaS), and many more. Thus, giving new way of providing services. These services can be in any form that is why known as XaaS and can be added as the part of SaaS.

2.1.5 Cloud Computing Deployment Model

The provisioning of the cloud services is being done in different ways. Pertaining to different deployment, managing, and operating policies, NIST has classified cloud computing deployment models as follows (Foster et al. 2008; Kavis 2014):

- *Public cloud*: These clouds are owned, managed, and operated by the third party that can be any government and business organization. These clouds are publically accessible and the IT infrastructure lies at the cloud provider's premises only. These clouds provide all the features of cloud computing, *i.e.* scalability, on-demand provisioning, and virtualization. But the data processing is carried out at the cloud provider end only. Entire control is in the hand of cloud providers only. The main limitations of these clouds are that they lack security of the confidential data, and problems like power failure, network issues can disrupt the function of the cloud. On the top of that, the main advantages of theses clouds are that they are more reliable and cheaper in comparison with the private clouds.
- *Private cloud*: These clouds are meant for single organization that can be used by the multiple users. These are owned, managed, and operated by the company only at their own premises. They have their own data centres and develop their IT infrastructure. These clouds are high-performance systems, and hold high-security measures for the confidential data. These clouds derived great benefits from the virtualization and automation. The third party can on and off visit the company's premises.
- *Hybrid cloud*: Hybrid clouds are composition of distinct clouds (private, public, and community cloud). These are the most economical models in the modern companies. But the difficulty lies in the smooth integration of the private and the public clouds environment. Main limitation of the hybrid cloud is the cloud bursting where the data from the private cloud burst into the public cloud.
- *Community cloud*: These clouds are designed to meet the requirements of specific community. The infrastructure may be owned by one or more companies, by third party or the combination of it. It involves the cooperation and integration of IT resources from the different organization.

With the increasing number of cloud consumers and application scaling challenges, it is very difficult for the single provider to meet the QoS requirement of the cloud users running their application at different geographical locations (Buyya et al. 2009). In addition, it is not possible for the single provider to establish their data centres at different location throughout the world (Bernstien et al. 2011). So, to meet the requirement of the users, multiple providers are coordinating with each other to form the federated cloud. To attain the seamless functioning of the federated cloud, well-structured management of computing, storage services, and network is required.

2.1.6 Limitations of Cloud Only Computing:

With the advent of more smart infrastructure coming in the existence, whether it is smart city, smart home, or more smart devices. As a lot of data has been started generating, cloud resources are turning to be limiting in many ways. Some of the limitations of the cloud computing are discussed as follows (Islam et al. 2013; Hartmann et al. 2019).

1. **Execution of the Redundant Data**

IoT sensor devices produce huge amount of data. To great extent, a lot of data is redundant, i.e. that data are not required to be send and store on the cloud in order to take any kind of action. For such instances, it is required to perform the execution locally at the lower level instead of cloud.

2. **Centralized Processing of the Data**

In the cloud, data from the multiple distributed sensor devices are processed on the centralized data centre. So data from the different regions cause congestion to the core network due to large volume of data.

3. **Difficulty with Low-latency Tasks**

In certain applications, like temperature measuring devices and streaming applications require fast processing of data. In cloud computing, communication between cloud resources and sensor devices takes lot of time that can cause failure of purpose of application. For e.g., disaster management system is time sensitive application which requires fast processing of the data.

2.2 Fog Computing and Its Applications

2.2.1 Definition of the Fog Computing

Fog computing is the distributed computing model that aims to bring the cloud near to IoT devices to minimize the energy required to communicate data from sensor nodes to the cloud. Communication will include three major steps: sending the data to the cloud, processing the data, and sending the response back to the sensor device (Bonomi et al. 2012; Yi et al. 2015). This communication consumes lot of sensor's energy. Fog computing is a distributed layer of multiple devices like: base stations between the sensor devices and cloud that performs the partial execution of the tasks near sensor devices to prevent the communication cost and save the battery life of the sensor nodes. As shown in the Fig. 2.1, fog computing layer lies between the cloud and sensor nodes. For the time sensitive applications where latency factor is counted a lot, there fog computing layer executes and stores the data temporarily and sends the data to the cloud layer for permanent storage.

The cloud layer consists of high-performance servers, performs the computation analysis, and permanently stores the data. These cloud resources are scalable and provide the resources on demand.

2.2.2 Six-Layered Architecture of Fog Computing

Like computer network layered architecture, fog computing also has six-layered architectures as shown below in Fig. 2.2 (Singh 2018).

Physical and Virtualization Layer: This layer consists of all the physical and virtual sensor nodes that actually acquire the data from environment and send to the layers above it. These sensors are distributed at different geographical locations.

Monitoring Layer: This layer is responsible for monitoring all the aspects relating to the processing of the tasks. This layer monitors the temperature, battery life, and the physical properties of the nodes.

Pre-processing Layer: This layer performs the cleaning of the unwanted data to reduce the processing time of the tasks at the moment. Data analysis in this layer also involves the mining of the relevant data from the large amount of data.

Temporary Storage Layer: In this layer, data are stored temporarily, till data are not stored permanently on the cloud. Many other operations are also performed on stored data on this layer like data virtualization, data distribution, and data replication.

Security Layer: This layer performs takes care of the data privacy, data integration, encryption, and decryption of the data at the fog computing level.

Transport Layer: This layer performs the uploading of the processed data to the cloud. The protocols used on this layer are light-weighted to save the energy of the nodes at the fog layer.

2.2.3 Characteristics of the Fog Computing

Fog computing carries different characteristics (Botta et al. 2016). Some of the characteristics are as given below:

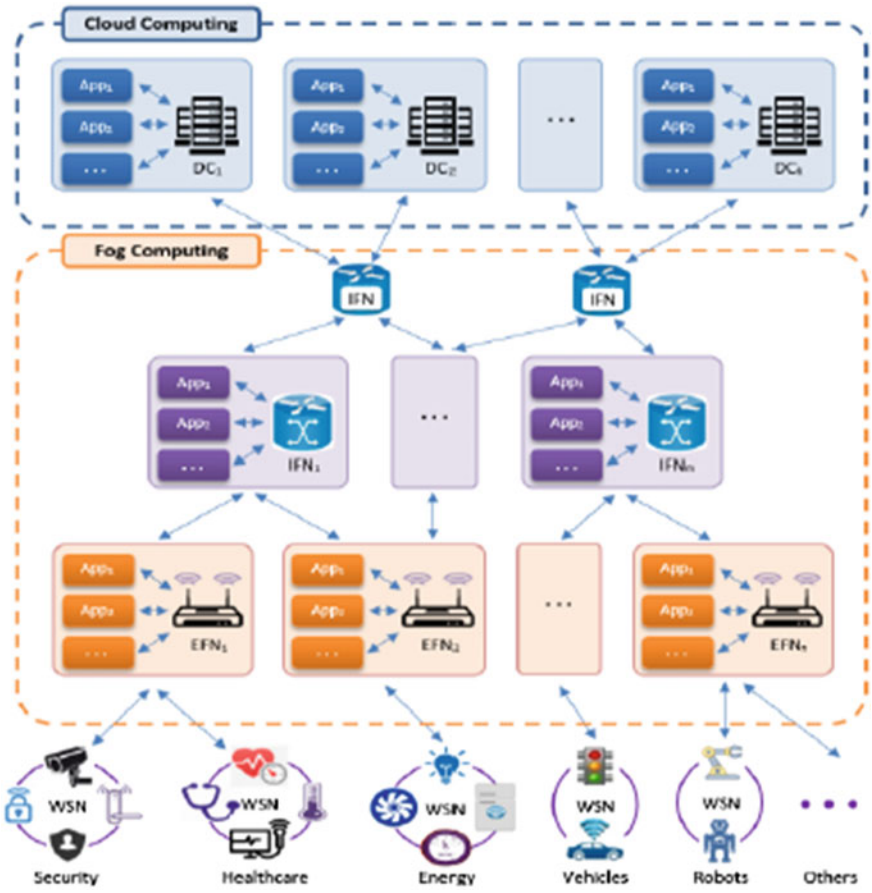


Fig. 2.2 Layered architecture of fog computing in IoT (Shah-Mansouri and Wong 2018)

Low Latency: In fog computing, since fog nodes are very near to the edge devices. It takes very less time to communicate and transfer data between each other. This feature helps the IoT devices to work efficient for time sensitive applications.

Geographically Distributed: In fog computing, the nodes are distributed amongst different geographical location, unlike to the cloud computing where computing resources are centralized, and all the execution of the tasks is done at centralized data centre only. They are placed in the close proximity to the sensor nodes.

Openness: Fog computing is loosely coupled, as it is compatible to multiple operating systems like Red-Hat, Ubuntu, Linux, Centos with different hardware configuration.

Heterogeneity: Fog devices are compatible to the different type of sensors nodes manufactured by vendors. Fog nodes are inter-operable on different platforms.

Flexible: Like cloud computing resources, fog resources are also flexible. With the increasing requirement, fog nodes can also be extended to reduce the burden on the fog nodes at the same level.

Characteristics of Fog Nodes:

1. **Storage**
2. **Computing facility**
3. **Network connectivity**
4. **Flexibility in the deployment**.

2.2.4 Locations of the Fog Node

In the fog computing, fog nodes are located at multiple physical locations. Fog nodes are meant to be present near the end sensor devices. Geographically, nodes can be present outside the hotel building, on the bus stand, street light, traffic light, and many more other different locations. It altogether depends on the placement of the sensor nodes. Broadly, the following are the broad classification of the fog node location.

1. **Gateway**
2. **Intermediate computer nodes**
3. **Network element such as routers**.

Under certain scenarios, like in the devices monitoring health, there gateway acts as an intermediate node between the sensors attached to the patients and the local servers. At some locations, like industrial environment, there router devices and cameras act as the fog nodes.

2.2.5 Application of Fog Computing and Its Role in the Internet of Things

Connected Cars

In order to operate the self-driving, there is connection amongst the cars and connection between the car and traffic light. Data from sensors attached to cars send the continuous data are processed by the nearby LTE mobile base stations to prevent the collision. At the same times, these cars also communicate with the traffic lights for the smooth governing of the traffic as sown in Fig. 2.3. Local processing is done at the fog only, and processed data are then sent to the cloud for further processing (Hartmann et al 2019).

Smart Traffic Lights

Fog computing in integrating with IoT devices can create smart traffic light management system, wherein traffic lights can communicate with adjoining nearby lights

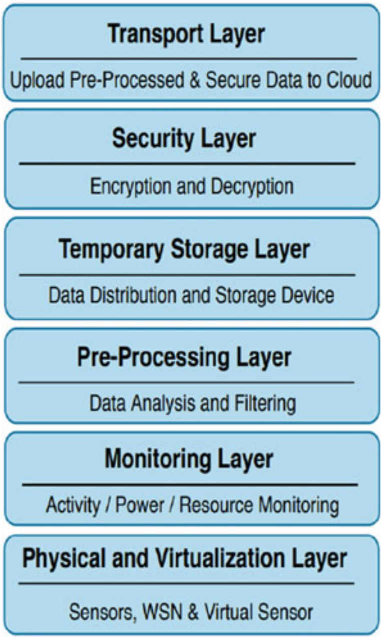

Transport Layer
Upload Pre-Processed & Secure Data to Cloud
Security Layer
Encryption and Decryption
Temporary Storage Layer
Data Distribution and Storage Device
Pre-Processing Layer
Data Analysis and Filtering
Monitoring Layer
Activity / Power / Resource Monitoring
Physical and Virtualization Layer
Sensors, WSN & Virtual Sensor

Fig. 2.3 Six-layered architecture of fog computing (Singh 2018)

other and can detect the traffic congestion on different and on the basis of that data can provide the smooth administration of the traffic. As shown in Fig. 2.4, with the help of vehicle detector control systems, it monitors the traffic of the vehicles and sends the control signals to the traffic lights. On the basis of these signals, nearby traffic lights communicate with each other for the smooth governing of the traffic.

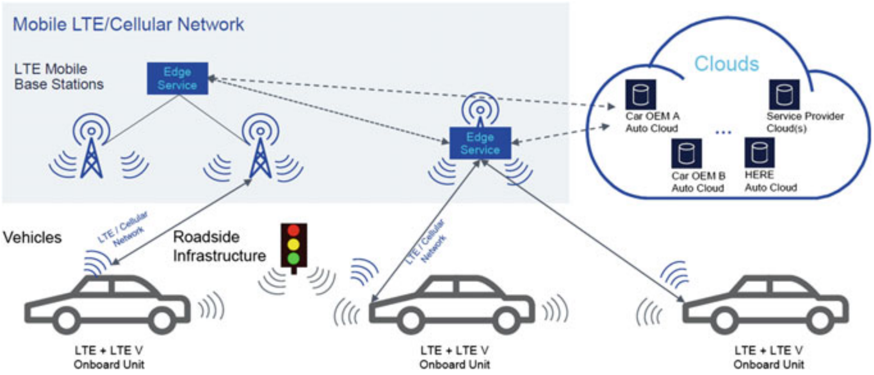


Fig. 2.4 Connected cars (Hartmann et al 2019)

Healthcare and Activity Tracking

In case of the medical field, wireless sensor devices have played a great role. Great amount of data is being generated by the sensor devices attached to the patients as shown in Fig. 2.5. A lot of data generated is redundant, need to be aggregated, pre-processed which otherwise have drained the storage devices. It is of no use to send the complete data to the cloud for the processing. So, fog computing layer performs all the pre-processing of the data and sends only the relevant data to the cloud for the historical analysis (Fig. 2.6).

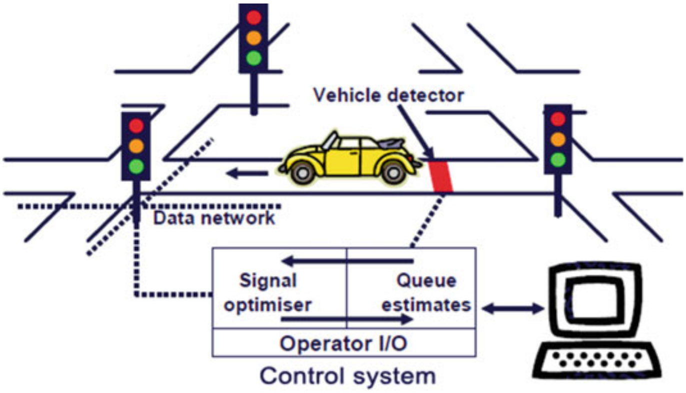


Fig. 2.5 Smart traffic light management system (Atlam et al. 2018)

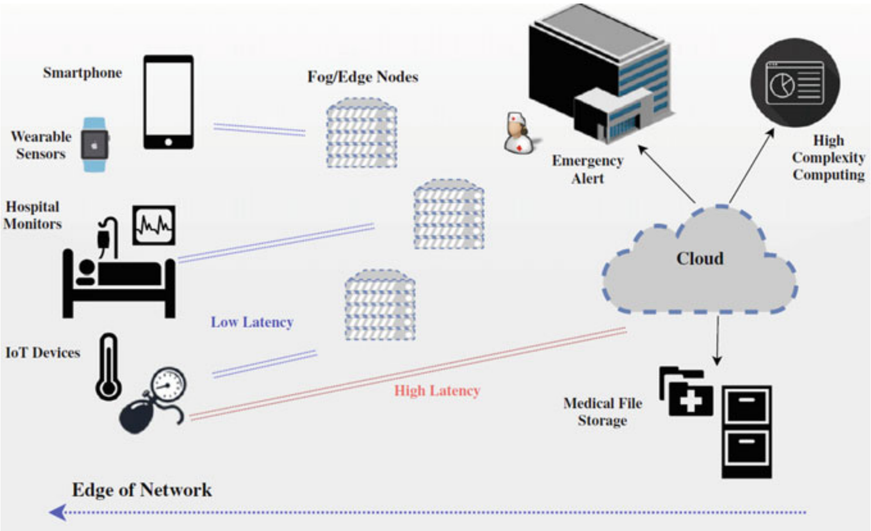


Fig. 2.6 Heath monitoring using fog computing (Hartmann et al 2019)

Augmented Reality: Popular augmented reality (AR) application like Google Glass required lager computation power and network bandwidth for processing the high-streaming data. Taking the example of the AR video application, it requires the fast processing of the data collected from the sensor nodes. That fast processing is not possible with cloud computing as processing delay of even the millisecond can cause the malfunctioning of the application. Multiple fog nodes are deployed at different locations within the city to make it smart city. These nodes consist of the sufficient processing, storage, and mining capacity for the real-time processing.

Mobile Big Data Analysis: Enormous amount of data from IoT devices is one of the major reasons of generating the big data. But due to serial processing of the data in the cloud, it takes time to process real-time data. There, federation of the multiple fog nodes can provide aggregation, high-computation power, and pre-processing of the data.

References

Atlam HF et al (2018) Fog computing and the internet of things: a review. Big Data Cognitive Comput 2(10):1–18

Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. ACM Press, New York

Botta A, de Donato W, Persico V, Pescapé A (2016) Integration of cloud computing and Internet of Things: a survey

Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I (2009) Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Fut Gener Comput Syst 25(6):599–616

Bernstien D et al (2011) An intercloud cloud computing economy—technology, goverence, and market blueprint. In: The proceedings of SRII Global Conference, IEEE

Foster I, Zhao Y, Raicu I, Lu S (2008) Cloud computing and grid computing 360-degree compared.

Galante G, Erpen De Bona LC, Mury AR, Schulze B, da Rosa Righi R (2016) An analysis of public clouds elasticity in the execution of scientific applications: a survey. J Grid Comput 14:193–216

Gupta P, Seetharaman A, Raj JR (2013) The usage and adoption of cloud computing by small and medium businesses. Int J Inform Manage 33:861–874

Hartmann M, Hashmi US, Imran A (2019) Edge computing in smart health care systems: review. Challenges Res Direct 33

Hartmann M et al (2019) Edge computing in smart health care systems: review. Trans Emerg Tel Tech 1–25

Islam MM et al (2013) Cloud computing: a survey on its limitations and potential solutions. Int J Comput Sci Iss (IJCSI) 10(4):159–163

Kavis MJ (2014) Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS), 1st edn. Wiley

NIST (2011) The NIST definition of cloud computing recommendations of the National Institute of Standards and Technology. Nist Special Publication

Rappa MA (2004) The utility business model and the future of computing services. IBM Syst J 43:32–42

Saxena S, Sanyal G, Sharma S, Yadav SK (2015) A new workflow model for energy efficient cloud tasks scheduling architecture. Second Int Conf Adv Comput Commun Eng 2015:21–27. https://doi.org/10.1109/ICACCE.2015.139

Shah-Mansouri H, Wong VWS (2018) Hierarchical fog-cloud computing for IoT systems: a computation offloading game. IEEE Internet of Things J 5:3246–3257

Singh P (2018) Cross-layer design for Internet of Things (IoT)-issues and possible solutions. Department of Systems and Computer Engineering, pp 1–10

Srivastava S, Saxena S, Buyya R, Kumar M, Shankar A, Bhushan B (2021) CGP: cluster-based gossip protocol for dynamic resource environment in cloud. Simul Model Pract Theor 108:102275. ISSN 1569-190X. https://doi.org/10.1016/j.simpat.2021.102275

Yi S, Li C, Li Q (2015) A survey of fog computing. ACM, New York

Zhang Q, Cheng L, Boutaba R (2010) Cloud computing: state-of-the-art and research challenges. 1:7–18

Chapter 3
Access Control and Authentication in IoT

Bhaskara Santhosh Egala and Ashok Kumar Pradhan

3.1 Introduction

The IoT devices are broadly classified as constrained and non-constrained based on their processing capabilities. The constrained devices are limited in computational resource capabilities and have minimal network connectivity. These devices come with pre-coded static operational instruction sets and less scope for the user or dynamic configurations. For example, smart lights, door and window sensors, temperature and humidity sensors come under this category. Because of limited processing capabilities, these devices mainly depend on a third-party computational service such as cloud computing for their data analysis. Moreover, they depend on intermediate gateways for secure communications with the remote cloud. In order to communicate with other devices, a variety of networking mediums such as wireless fidelity (Wi-Fi), short-range wireless technologies (Bluetooth and near-field communication (NFC)), and cellular networks are employed. The non-constrained devices, on the other hand, or self-reliant and have the necessary data storage and processing capability. They perform basic data operations to make primary decisions for actuators. Further, they communicate with the cloud for high computational and data storage operations. Though these devices are more capable, they still depend on manual configurations to operate. At the same time, the improper configurations and default devices configurations lead to cyber-attacks. Also, both category devices do not have whole-level security mechanisms by default and come with limited configurations. In order to protect these devices from cyber-attacks, we need more specific and lightweight mechanisms. Most of these mechanisms point to the need for identity management and access control. Deploying device-specific security mechanisms is not worthy if we need to maintain a vast number of IoT devices. One compromised device weakens total system security. In 2016, a complex distributed denial of service (DDoS) attack was initiated on a well-known security service provider's

B. S. Egala · A. K. Pradhan (✉)
SRM University, Amaravati, Andhra Pradesh, India
e-mail: ashokkumar.p@srmap.edu.in

B. S. Egala
e-mail: bhaskara_santhosh@srmap.edu.in

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_3

website using the Mirai IoT botnet (Antonakakis et al. 2017). The recent security breaches highlight the necessity of multilayer security for IoT devices to guarantee their security and privacy levels to combat future attacks. This layer filters most of the cyber-attacks and minimizes the effect on the IoT system operations. We can use intermediate gateways and public cloud computing to deploy these layers. In this chapter, the primary security breach surface vectors and identity management mechanisms are highlighted in Sect. 3.2. Authentication mechanisms to support privacy features in the IoT ecosystem are discussed in Sect. 3.3. We have given a brief introduction to the access control mechanism in Sect. 3.4.

3.2 Identity Management in IoT

Every device in the IoT ecosystem requires a unique identity in order to implement security rules. Devices can use strong identity management to identify themselves before establishing a secure connection with other devices and users. A typical device life cycle of activities includes identity formation at the design device, device registration at manufacturing, assigning deployment certificates for field deployment, identity parameter maintenance, and revoking or terminating identity parameters of the device.

- **Identity at Designing-Stage**: The initial stage in the identity creation and management of IoT devices starts with the designing stage itself. Every device gets an essential identity in the development stage and flashes to its ROMs for future deployment. The identity is mainly related to manufacturing and device unique manufacture identity and essential certificates for secure operations. Since most IoT devices are not updated with security patches throughout their lifetime, the design stage places a more significant role in device identity management. Besides the heterogeneous nature of manufacture designing policies, it becomes too challenging to use manufacture given identity to control the IoT ecosystem.
- **Deployment**: The primary identification of the device is used to register it locally, and a secondary identity is produced. In addition, depending on the deployment, devices are classed as Brownfeaild or Greenfeaild. A single corporation or organization can only use the secondary identity. A set of specialized cryptography settings is also included in the deployment. When a device enters a live state, these values are utilized to send or receive data from other devices. It streamlines the organization's auto-identification procedure.
- **Manage**: To extend their life and functionality, deployed devices are subjected to continual monitoring or device management. The credentials and crypto parameters are renewed or revoked at this step, depending on the circumstance. Any device's identity gets extended or destroyed as a result of this. Furthermore, secure over-the-air (OTA) updates are sent regularly to ease device administration and enable automation. This step includes ownership transfer, certificate renewal, reporting, and logging.

- **End of Device life**: An IoT device's last step likewise serves as the final stage of its identification. The gadget is zeroed when the identification has been received. To reduce the attack surface, it is critical to revoke certificates and security credentials. Attackers have been known to utilize the revoked or fabricated identities of zeroization devices in the past. As a result, the revocation and identity management system should be designed to identify and prevent counterfeit identities. Figure 3.1 illustrates the normal identity management life cycle in IoT ecosystem.

The different identity management coupling methods are depicted in Fig. 3.2. The coupling of identity in the same domain is simpler and more manageable, whereas different domains with weak identities are challenging.

Furthermore, the sort of protocols and services that the device uses to interact on the Internet may generate the device's identity. We may further divide identity into two types: physical identity and virtual identity. Physical identity refers to the hardware characteristics that distinguish devices, such as the media access control (MAC) address and defined communication settings. Radio frequency identification (RFID) is an example of a radio wave system to show its identification. The constrained application protocol (CoAP) is intended to allow HTTPS-based restful IoT apps. The current IoT devices are not self-protective from identity theft attacks; moreover, they depend highly on physical identity than virtual identity in industry 4.0 use-cases. These are inconvenient and unsuitable for IoT ecosystem privacy and security in real time. As a result, keeping one's identity hidden from the outer world is essential. A defined namespace is a superior choice for hiding a device's existence on the internet. Identity lifecycle design also includes establishing extensible identity management, identifying the needed security methods, and clearly defining privacy policies for various data species. The deployment procedure should begin

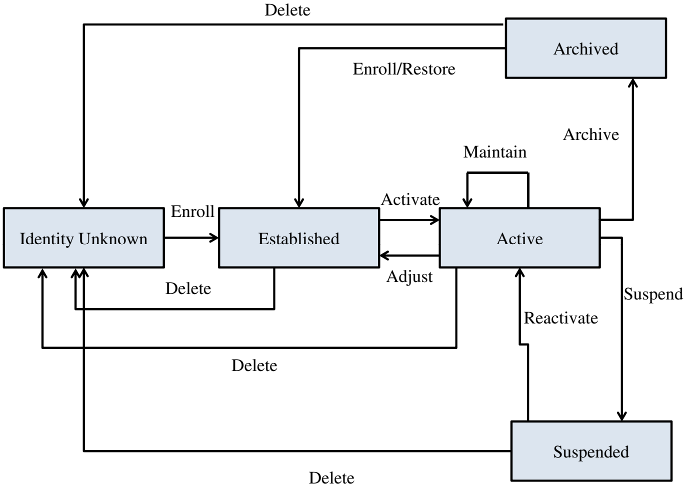


Fig. 3.1 Identity management life cycle in IoT ecosystem

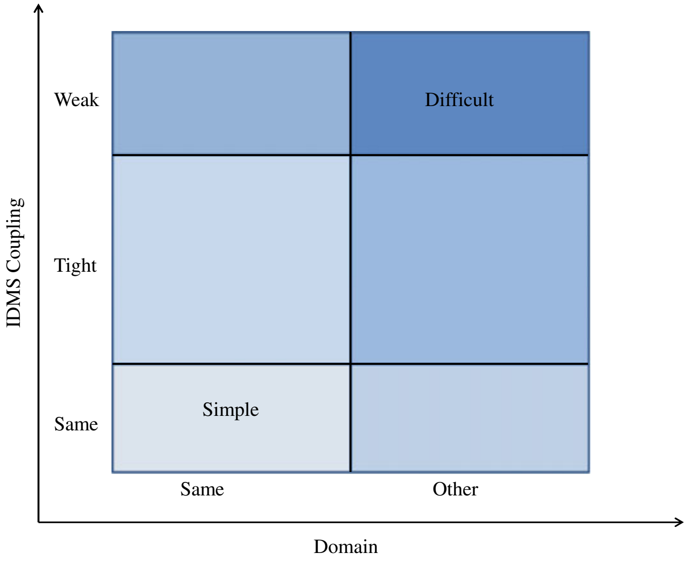


Fig. 3.2 Identity management systems coupling in IoT ecosystem

with resetting the default passwords to protect devices against assaults. In multicasting use-cases, an identity might refer to a collection of devices and an entity can have several identities (Dib and Toumi 2020).

3.2.1 Inter-domain Identity Management Architectures

IoT virtual identity management is a particularly significant operation in inter-domain identity management architectures. Figure 3.3 shows an inter-domain identity network operation structure in which individual identity management systems are collectively accountable for directing a specific network-level identity. The structure may be improved by incorporating scale scenarios with intermediate coordinating identity management subsystems (IDMSS).

Figure 3.4 showcases an alternate standard structure in which various IDMSS collaborate on a peer-to-peer basis. In this architecture, not every IDMSS system will interact with others in the network to form the network-level identity. Only one peer takes responsibility for formulating the identity using the remaining IDMSS systems information.

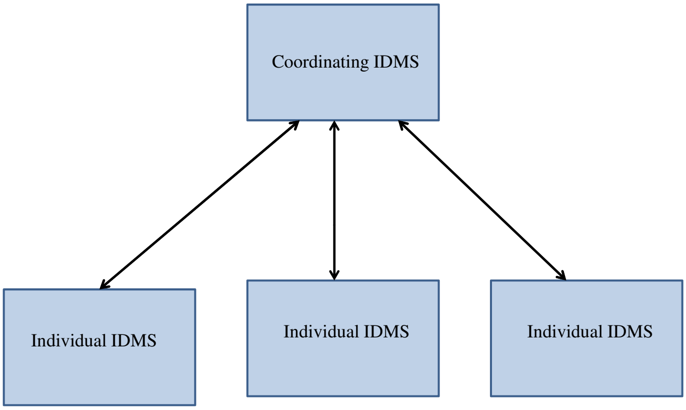


Fig. 3.3 Centrally coordinated IDMSS network

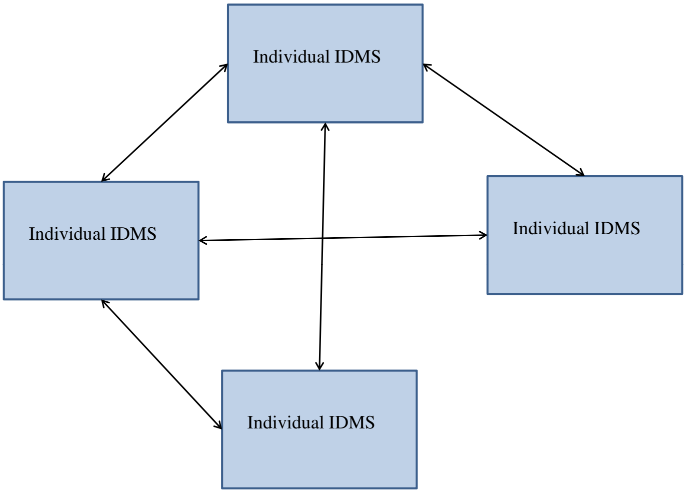


Fig. 3.4 Peer-to-peer coordination

3.2.2 Techniques to Build a Coordinating System

While developing a coordinating system for inter-domain identity management introduces technical and management issues because of ambiguity in IDMSS level operations. As shown in Figs. 3.3 and 3.4, every subsystem should share its local identity information over the TCP/IP layer with a central coordinating system. The network-level identity is an agreement between the subsystems and coordinating system to validate the new identity throughout the network (Jia et al. 2020).

3.2.3 Single Sign-On Identity Federation

When it comes to forming identity coalitions, single sign-on (SSO) (Teravainen 2020) is a frequently requested feature, especially when people are involved. SSO enables the use of a reality's identity in one sphere to authenticate a reality in another. SSO's purpose is to assist in dealing with individualities in two or more disciplines simultaneously. The identity confederation agreement has completely automated protocols and processes for data processing and interchange among disciplines. Enterprise and pall system designs can be seen using cryptography-based identity coalitions to offer SSO services. Some of the most widely used authentication protocols are SAML (Ferdous and Poet 2013), OpenID (Recordon and Reed 2006), and OAuth2.0 (Fett et al. 2016). The SSO protocols allow humans and IoT devices to consume digital services by maintaining identity and trust between multiple actors. It reduces the burden on people and devices by eliminating the requirement of remembering the credentials all the time. The simplified examples where we can use these methods are as follows.

3.2.3.1 Network-Level Service for Nodes Communication

A lightweight M2M (LWM2M) operation protocol is used to send and receive data to and from other service devices and operation services. Because the quantity of services utilized is largely constant during the lifespan of the IoT device, and there is no mortal convenience advantage, an SSO-able identity confederation is not required in this situation. Using business SSO protocols on tiny IoT devices, on the other hand, adds a tremendous amount of complexity to the device firmware. When SSO is required on an IoT device, Featherlight SSO protocols should be investigated instead. Mahkonen et al. (2013) is a mobile network technology that permits an identity from one province to be reused across many disciplines. Using mobile network subscribers' individualities, relevant key cryptographic material, and cryptographic algorithms, the GBA structure provides a transient, cryptographically secured link between an IoT device and a service in the operation layer. Before granting service access, the security association may conduct conditioning, such as authenticating the IoT device. For mobile networks, a GBA uses well-known identity information suppliers (IIPS). The IoT gadget operates with a GBA-compatible SIM such as a universal integrated circuit card (UICC)/embedded universal integrated circuit card (eUICC) (Smeets 2019). Despite the fact that the 3GPP identity and GBA are now connected with cellular networks, this technology may connect non-3GPP items to a network. In this case, attack-specific sequestration and protection methods may be utilized to safeguard the corresponding credential and supporting software, avoiding the use of UICC in IoT devices.

3.2.3.2 Mapping

The strength of SSO is entirely dependent on its cryptographic mechanisms; in SSO operations, no data about participant identity, security keywords, or cryptography methods are exchanged with other participants. Still, this is not the only way to create a confederation of identities. Another popular method for forming an identity federation is mapping. The identification of one field is counterplotted with the identity of another. The mapping can be carried out precisely as written or with slight changes. The mapping process contains adding redundant identity data to respective original identities in a synchronized passion from multiple locations in the entire day. A communication machine is a software structure used for communication and event exchange among IDMSS. Regardless of whether these two mapping methodologies are used, simultaneous changes to the counterplotted data in the linked disciplines must be addressed. By designating one field as the master for particular identity data, this may be prevented. Two distinct techniques of solving issues with tracking and syncing idenitities are three-way merging and differential synchronization. The IDMSS ecosystem might be modest or large, and it can contain a few or many different forms of identifying data. Figure 3.5 depicts four identity operation disciplines, each of which abstractly embodies the technological and organizational characteristics of an IoT system.

- **Service User Domain(SUD)**: The location where the Internet of things registrars identity and operates.
- **Service Management Domain(SMD)**: The location where the IoT device's operation or services are linked to business operation waiters who handle freight data.

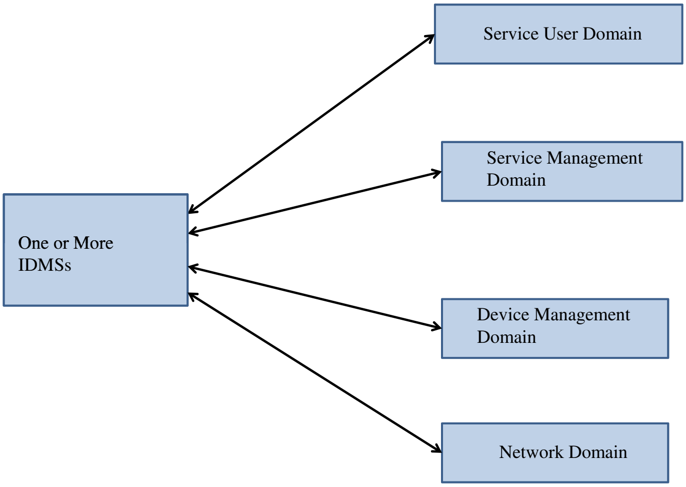


Fig. 3.5 IMDs in the IoT

- **Device Management Domain(DMD)**: Services based on the LWM2M protocol to manage essential device functions such as the device lifecycle and firmware or operating system.
- **Network Domain(ND)**: The network domain (ND) describes how IoT communication takes place, for as through a cellular network or another sort of wide area network (WAN) or a local area network (LAN). In the Internet of things, there are four distinct identity management domains (IMD) as represented in Fig. 3.5.

3.3 Authentication Mechanisms in IoT

Convention authentication and authorization approaches are ineffective due to many IoT heterogeneous nature and different machine-to-machine communication characteristics. For dispersed IoT settings, experimenters in Xu et al. (2018) presented a capability-grounded access control paradigm. It allows groups to participate in a single commemorative and uses IPsec to give end-to-end security. A panhandler can communicate with any device in a group using a single commemorative for group access. The network prefix unique original identifier is used to construct an access group identification (ULA). A ULA identifies each device in the group. The panhandler in a group access commemorative has its ULA and the network prefix of the access group. As a result, the commemorative's ULA and prefix may be used to authenticate the groups of objects. It can also provide admission if the panhandler has a ULA commemorative. Cruz-Piris et al. (2018) is an OAuth2.0 profile that allows vivid agents to have multiple access requirements, according to the Stoner-Managed Access paradigm. "SmartOrBAC," based on the OrBAC paradigm, was presented as a unique access control architecture for an IoT environment in Pasquier et al. (2015). Web services were employed to operate the security applications in this method. We have a variety of models based on parameters and operation style. In this part, just a few of them are examined in depth.

Though the classical OrBAC works best in a centralized system, it lacks collaboration capabilities and security conversion mechanisms. For that reason, a SmartOrBAC is introduced to get around these limitations. The work in Pereira et al. (2014) suggested a novel access control structure for power-constrained devices. It combines the principles of Kerberos and RADIUS access control systems to provide a dependable access control framework. In order to achieve low-power access control and authentication, it barrows and combines features of Kerberos and Constrained Application Protocol (CoAP). A lightweight, secure, and scalable IoT group authentication protocol named threshold cryptography grounded group authentication (TCGA) is introduced by Mahalle et al. Mahalle et al. (2014) to simplify the group authentication process. Group authentication reduces the handshake's outflow, resulting in lower resource use and energy savings. TCGA successfully eliminates man-in-the-middle attacks over IoT networks. Tomanek and Kencl (2016) demonstrated a method for ensuring the security of a smart home system using the AllJoyn framework and uses elliptic curve cryptography to authenticate users. Lee et al. 2014 proposed the lightweight authentication technique by upgrading the original RFID system security basis for IoT. Current RFID systems do not use encryption for authentication, which is a security flaw. A lightweight cryptographic system based on the XOR technique that employs encrypted passwords for authentication is proposed to solve this problem. Existing certifications rely on signatures, which are difficult to apply on resource-constrained IoT devices. A confirmation code, on the other hand, is straightforward to maintain in an IoT setting. Zhao et al. 2011 introduced an asymmetric mutual authentication system for the Internet of things that performs authentication between the terminal node and the platform. Both SHA1 and feature extraction are used in the proposed method. As a result, IoT security, as well as computation and transmission costs, have decreased.

3.4 Access Control Models with Examples

As the backbone technology for ensuring information security, access control opens up possibilities for addressing the IoT's difficulties mentioned above. Access control can efficiently monitor resource access and prevent illegal data flow. However, because IoT search is a relatively new study topic, standard access control methods and approaches cannot adequately tackle IoT search's access control issues. The following are the aspects of data access in the IoT search environment. Figure 3.6 illustrates the IoT ecosystem access control taxonomy in very abstract form.

- **Massive**: According to a 2011 analysis, M2M traffic in the USA grew by 250 percent and estimated that it would cross the total Internet users count by 2020. As per the latest reports in 2021, nearly 25 billion devices are connected with a speed of 9. 127 new devices every second. These devices generate massive amounts of data which introduces new issues in data management and utilization.
- **Dynamic**: Nodes and users often change in the IoT search environment, and access objects are frequently added and removed. Because of its dynamic nature, it is impossible to forecast all user information ahead of time and correctly comprehend the user and permission structure.
- **Strong Privacy**: Data privacy and security have become increasingly crucial as data sharing has progressed. Many privacy proposals, such as ISO/IEC 29100:2011, privacy by design, global data protection law, and fair information practice principles, have been suggested by governments and researchers to safeguard an individual's privacy. On the other hand, many academics wonder whether these principles have aided privacy because some of them emphasize individual control over data rather than data security.
- **Multiparty Commonality**: Data is no longer restricted to a single or closed environment in IoT search; instead, it is created and shared by a number of cooperating entities. Multiple dynamically connected information systems make up the IoT search service. Information is transferred and shared across partnering firms to meet the complex application needs.

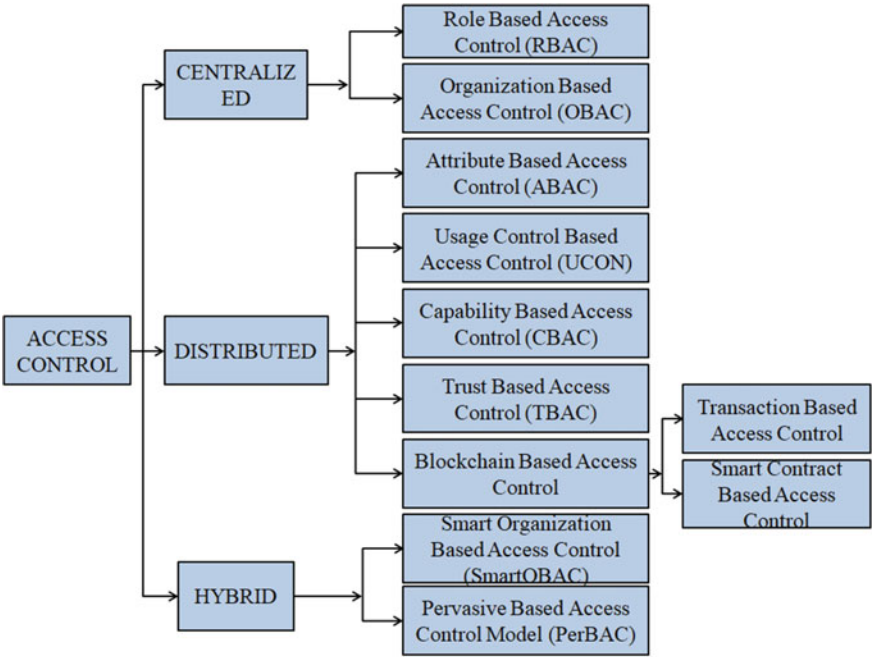

ACCESS CONTROL
CENTRALIZ ED
DISTRIBUTED
HYBRID
Role Based Access Control (RBAC)
Organization Based Access Control (OBAC)
Attribute Based Access Control (ABAC)
Usage Control Based Access Control (UCON)
Capability Based Access Control (CBAC)
Trust Based Access Control (TBAC)
Blockchain Based Access Control
Transaction Based Access Control
Smart Contract Based Access Control
Smart Organization Based Access Control (SmartOBAC)
Pervasive Based Access Control Model (PerBAC)

Fig. 3.6 Access control taxonomy

Access control mechanism monitors and controls the resources access and utilization based on the defined rules. It acts as the primary security mechanism when maintaining data confidentiality and privacy. Standard access control methods and approaches, on the other hand, are unable to fully address the access control difficulties that IoT search meets because it is a relatively new study area. To achieve specific goals, data is constantly exchanged and shared among devices and people in the IoT ecosystem. In this shared environment, authentication, secrecy, and access control are all required for safe communication. In this shared environment, authentication and secrecy are required to build a secure communication system. How can the edge device verify that the query or command coming from the authorized device is genuine? To ensure authenticity and secrecy, public-key cryptography, signatures, and authentication are commonly utilized. Access control is applied to the data stream in the IoT environment rather than the traditional database management system. Ensure access authorization, managing the scalable IoT architecture, handle a large amount of data stream are some of the access control issues in this case.

By the 1970s, access control schemes like the BLP model and the Biba model Jin and Shen (2012) were primarily used in mainframe systems. The BLP idea is based on a military security approach that addresses hidden hierarchical information access management challenges. It is the first rigorous theoretical proof of a mathematical access control paradigm. In 1975, Kenneth J. Biba created the Biba model. The formal state transition system of a computer security policy establishes access control rules for maintaining data integrity. The Clark–Wilson model Vimercati and Samarati (2011) was published by Clark and Wilson in 1987 to track and audit the subject's state transition as well as the low-watermark policy parameters' runtime alterations. In contrast to Biba, the Clark–Wilson approach uses controlled state transfers to offer comprehensive integrity protection. The Biba model, on the other hand, provides a main multilevel integrity access control mechanism, but it cannot be used without the existence of a trusted subject. As the criteria for computer trustworthiness expanded in the 1980s, research recommended for more flexible access control techniques.

One of the most typical works is the US Department of Defense's trustworthy computer system assessment criteria (TCSEC) (DoD). TCSEC is a standard that specifies the core criteria for assessing the efficacy of security systems. TTCSEC divides access control into two categories depending on the tasks of access authority users as discretionary access control (DAC) and mandatory access control (MAC). Legal users can access objects as individuals or organizations under the DAC paradigm, but illegitimate users cannot. Due to the high level of administrative complexity, DAC must manually manage users, authority, and resources, making it inappropriate for IoT search. A central authority can use the MAC model to assign access rights based on regulations. This category includes policies from both the business and public sectors. In MAC applications, a multilayer security architecture is widely utilized. Despite the fact that the MAC approach overcomes the problem of decentralized resource management by centralizing permission management, it is inefficient for IoT search users.

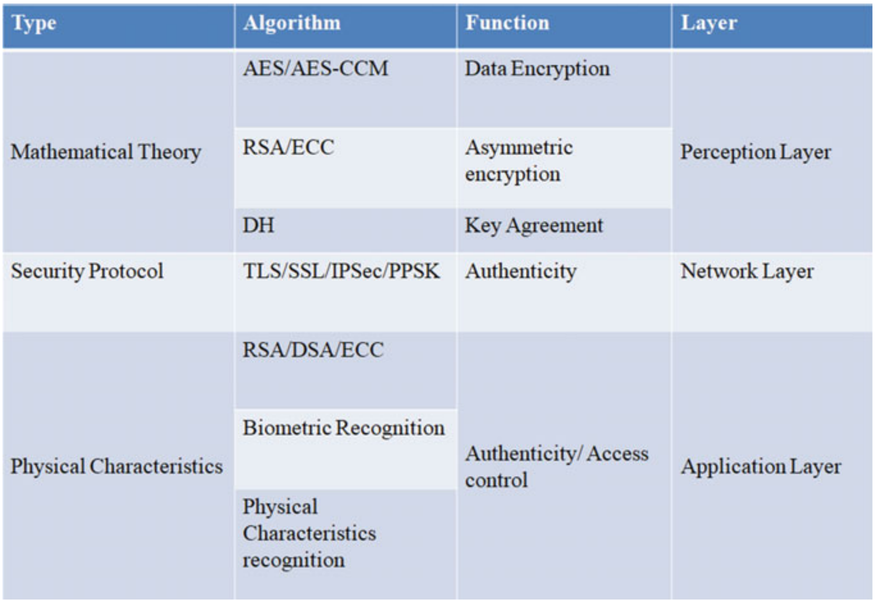
With the introduction of the Internet and the proliferation of large-scale applications of information systems in businesses around the year 2000, traditional access control models like DAC, MAC, and their extension models struggled to handle sophisticated application layer access needs. It was advised to adopt a role-based access control (RBAC) (Sandhu 1998), which limits system access to authorized users. Role permissions, user roles, and role linkages are all components of RBAC that make user assignments simple. RBAC may be used in large corporations to ease security administration and verify that information systems meet information integrity standards. In contrast to MAC and DAC, RBAC can execute these requirements without generating any problems. Access control technology-based applications face substantial challenges when new computer environments emerge, such as Internet of things (IoT) search. DAC, MAC, and RBAC are examples of closed environment approaches incompatible with current computer settings. ABAC Kolter et al. (2007) defines access control rules based on different attributes and environmental attributes, based on the combination of attributes resources or services are allocated or denied.

Ferraiolo et al. (1999) presented RBAC in 1992, a role-based access control system. Unlike traditional access control models, which require a system administrator to assign responsibilities, ownership manually, or security labels to users and objects, ABAC allows users and objects to define access policies based on existing attributes. Because characteristics may represent objects from numerous viewpoints, users can alter access control strategies based on actual circumstances. TRBAC (Bertino et al. 2001) is a temporal RBAC modification that leverages triggers to allow for recurring role enabling, disabling, and temporal dependencies via triggers. Along with time data, location limits must be handled in the IoT environment. When access to resources involves taking into account both time and location information, researchers have proposed spatiotemporal RBAC (STRBAC) (Geepalla et al. 2013) as a high-level concept of access control. Meanwhile, the creators of (Park and Sandhu 2004) developed concept utilization control (UCON), which enables for finer-grained regulation of digital object utilization than standard access control rules and models.

The features of access control entities influence ABAC's access control decisions. Subject attributes, object attributes, permission attributes, and environmental attributes are frequently expressed as four tuples. Although ABAC provides users with a great deal of control over their access to resources, personal data security is not considered. Studies suggest attribute-based encryption (ABE), which encrypts objects based on attribute-based access limits, based on the notion of classical ABAC.

Well-known ABE variants are key policy-based ABE (KP-ABE) (Attrapadung et al. 2011) and cipher-based ABE (CP-ABE) (Porwal and Mittal 2017). In KP-ABE, the policy is linked with the user's private key, whereas in CP-ABE, attributes of the policies are encrypted with the help of the user's private key. The KP-ABE is an inverse form of CP-ABE, where in the first user, freedom is relatively strong. In contrast, data owner freedom is decreased and coming to the second, the data owner determines the access control policy, which gives additional control to the data owner. Figure 3.7 presents a holistic comparison of well-known access control models.

- **Based on ABAC**: All qualities linked with characteristics are used to identify the person and the object. When a user submits an access request in the ABAC model, he is given the appropriate access permission based on his characteristics. Recent research has concentrated on the concept of preserving user privacy since attributes may include users' private information, which, if leaked, would substantially hinder the development of ABAC. Xu et al. introduced the privacy-preserving ABAC (P-ABAC) method. The sensitive characteristics in the P-ABAC are handled using homomorphic encryption on the user's side.
- **Based on RBAC**: The RBAC model defines user responsibilities, privileges, and administrative functionalities as access rules and separates the underlying user tasks. It mainly suffers from role explosion over multiple domains due to improper access rules management. An improved model named service-based RBAC paradigm was proposed by Spiess Patrik (Jindou et al. 2012) to support IoT applications task-based access controls with the help of RBAC. An enhanced RBAC model employed by Zhang and Tian 2010 utilizes the context rules in order to deliver a more scalable, flexible, and lightweight access control mechanism.
- **Based on CapBAC**: In the CapBAC model, however, access control is the user's responsibility. A BlendCAC model, which is a blockchain-enabled decentralized CapBAC, was proposed by Xu et al. 2018. The BlendCAC approach, which leverages a smart contract for access authorization registration, propagation, and revocation, proposes a strong identity-based capability token management technique.



Type	Algorithm	Function	Layer
Mathematical Theory	AES/AES-CCM	Data Encryption	Perception Layer
	RSA/ECC	Asymmetric encryption	
	DH	Key Agreement	
Security Protocol	TLS/SSL/IPSec/PPSK	Authenticity	Network Layer
Physical Characteristics	RSA/DSA/ECC	Authenticity/ Access control	Application Layer
	Biometric Recognition		
	Physical Characteristics recognition		

Fig. 3.7 Security policies literature comparison

A cloud-based authentication framework was proposed by Barreto et al. (2015). Users can use the IoT cloud to manage various intelligent pervasive environments by accessing IoT-based resources and capabilities. In large-scale IoT systems, a federated CapBAC (FedCAC) (Xu et al. 2018) framework presented a strategy for managing identity-based capability tokens, which includes registering, propagating, and revoking access.

- **Based on UCON**: While active user access is active, the UCON model provides a wide range of access qualities by enabling given access to be withdrawn and use to be terminated. UCON is an innovative and promising access control solution for open, distributed, heterogeneous, and networked computer environments. The PEI, a UCON-based security framework that takes a tiered approach to policy, enforcement, and model implementation, was introduced by Zhang et al. (2010). The policy model layer specifies predicates on subject and object properties, system attributes as conditional restrictions, and user actions as obligations.
- **Organizational-Based Access Control (i.e., OrBAC):** In order to form OrBAC, a new dimension called "organization" is added to the existing RBAC paradigm. OrBAC is enhanced by the Trust-OrBAC paradigm, which adds the idea of trust management. With various options, Trust-OrBAC provides two dynamic trust vectors, one for organizations and one for users. The Tr-OrBAC paradigm, which combines Trust, increases cross-organizational collaboration while avoiding malicious activity. The SmartOrBAC concept broke down the challenge into layers. SmartOrBAC divides processing expenses across limited and unconstrained devices.

- **Blockchain or Biometrics Features based**: Because of the diversity of IoT devices, bio-characteristics are increasingly becoming one of the most important factors used to authenticate IoT devices and their users. Ferrag et al. (2019) looked at the biometrics utilized by authentication and authorization techniques for mobile IoT devices, such as voice, fingerprints, and other biometrics. FairAccess for IoT is a blockchain-based access control architecture presented by Ouaddah et al. (2017). New transaction types for giving, gaining, delegating, and canceling access are introduced in FairAccess. In FairAccess, the access token is required to access a protected resource, but it cannot be triggered until the access control conditions have been met. The real-time and bloat blockchain issues are the primary limitations of FairAccess when using the UTXO architecture of blockchain. In recent times, the authors in Egala et al. (2021), Egala et al. (2021) introduced a selective sharing access control mechanism for decentralized IoT medical and time-critical applications. It presents a holistic view of security architecture for time-critical IoT applications.
- **Open Authorization (i.e., OAuth)**: OAuth is a client-side access control mechanism for web server resources. The majority of traditional web and cloud application solutions are incompatible with the context environment. The OAuth-IoT framework was suggested by Sciancalepore et al. (2017) for access control. OAuth-IoT takes advantage of current open standards and harmonizes them correctly. For proper application authentication and authorization, OAuth-IoT natively supports any token format. Fernández et al. (2017) developed an OAuth paradigm for application-scoped authorization that allows controlling roles and permissions. OAuth 2.0 makes authorization incredibly light for all the essential information that is supplied with a token.

3.4.1 Open Challenges

1. **Policy Conflict Due to Fragmented Authorizations**: Several IoT access control solutions are available, the majority of which highlight the importance of integrating inter-domain access controls to form network-level controls. Nevertheless, they believe that a single entity governs resources by ignoring the multiparty sharing feature. Always considering multiple local rules may increase conflict in generating system-level access rules because of deviations in fragmented rules. Several techniques use an essential strategy to address this issue, such as approving access only when all users agree. This strategy, however, is too restrictive to be used in real-world applications since it would limit resource availability. More work is needed to focus on policy conflict resolution caused by varied authorizations, enhancing policy composition, and automating conflict resolution.
2. **Policy Conflict Due to fragmented Relationships between parties**: This sort of policy conflict arises due to the particular characteristics of the IoT search environment. In the process of integrating multiparty access control policies, the rules of multiple agents include several constraints. Access to the same resource

may be restricted differently by multiple owners. Based on these limits, several access control decisions that correspond to each resource may be derived. Each ace control option may be tailored to the needs of different users. However, the options may be mutually exclusive. Inconsistencies and disagreements are common when these constraints are combined. As a result, figuring out how to choose and update access control options for different users quickly and dynamically is a serious issue that must be solved.

3. **Attribute-Permission Assignment Within Noisy Data**: The Internet of things (IoT) search engine is a collaborative ecosystem that spans several domains. Distinct domains have different access control policies. Because attributes are essential, and the access control decision is made based on the set of attributes of the requester. Every non-ABAC access control model must be converted to the ABAC model to achieve unified administration of an access control policy. ABAC is well-suited to the IoT search context because it separates the policy administration from the access control decision. Moreover, ABAC requires a pure and quality correlation between attributes and permissions to migrate from role-permission and user-permission relationships. Noise data, in particular, is frequently included in the initial user-permission relationships, affecting policy generation accuracy and posing significant security threats to access control systems. A significant research problem in controlling access for IoT search is how to manage attribute-permission assignment inside noisy data.
4. **Modeling and Evaluation of IoT Security Search**: As the Internet of things (IoT) has grown in popularity, so has its security. In recent decades, many similar complex security challenges have been effectively solved using modeling and simulation (MS). MS approaches and tools are also helpful in tackling IoT challenges since IoT has a unique address and communicates using conventional communication protocols. However, modeling and evaluating IoT security searches have received little attention.
5. **Things authentication and anonymity in IoT**: In the subject of industrial control security IoT, many authentication mechanisms aiming at real-time communication between the cloud platform and sensing devices are being developed. However, these approaches' efficacy and security cannot always be ensured at the same time. More emphasis should be placed on device authentication and anonymity protection technologies to ensure the data source's reliability, privacy, and data availability.

3.4.1.1 Addressing Risks

There is no distrusting that IoT security is too complex, but experts in the area are well-clued in the stylish ways for practical threat assessment and compensating reduction. Expert cooperation makes IoT installations a breath. One of the crucial ideas is that security must be inaptly regarded right at the launch of the design process, inside the professional moxie stationed as soon as possible—indeed from outside the business if needed. There is no question that this procedure leads to increased security.

The longer the process of critically analyzing, testing, and hardening IoT results is held up, the more delicate and precious it becomes to do it right the first time. Worse yet, chancing significant excrescences or inadequate contingency medications after a suspected breach has formerly passed can be far more expensive.

According to Juniper Research's Star Critic Steffen Sorrell, cybersecurity in IoT is crucial. For enterprises, the first political step is to develop safety from the ground up, focusing entirely on the fundamentals. Consider the secure element as an example. It is possible to attach it to the device and use it to carry out cryptographic procedures. In the security chain, the tackle security module is an often duplicated critical tackle item (HSM). Structure protection from exposure is the first political step for businesses. We need to think about security holistically from the ground up (devices, networks, applications, infrastructure) regarding how they can be secured moment and in the future. The three pillars that uphold connected things and services must be defended as an overall cybersecurity strategy.

- Confidentiality,
- Integrity,
- Availability.

It is a matter of designing applicable security within the three security pillars to guarantee that their pretensions are met. Companies may help unauthorized access to data, things, and software by espousing recommended security results, similar as device and authentication operation results grounded on encryption ways, as soon as possible, with expert knowledge applied.

References

Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, Durumeric Z, Halderman JA,Invernizzi L, Kallitsis M, Kumar D, Lever C, Ma Z, Mason J, Menscher D, Seaman C, Sullivan N, Thomas K, Zhou Y (2017) Understanding the mirai botnet. In: Proceedings of the 26th USENIX Security Symposium

Attrapadung N, Libert B, de Panafieu E (2011) Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Catalano D, Fazio N, Gennaro R, Nicolosi A (eds) Public key cryptography-PKC 2011, Berlin, Heidelberg. Springer, Berlin, pp 90–108

Barreto L, Celesti A, Villari M, Fazio M, Puliafito A (2015) An authentication model for IoT clouds. In: 2015 IEEE/ACM International conference on advances in social networks analysis and mining (ASONAM), pp 1032–1035

Bertino E, Bonatti P, Ferrari E (2001) Trbac: a temporal role-based access control model. ACM Trans Inf Syst Secur 4:191–233

Capitani De, di Vimercati S, Samarati P (2011) Clark and Wilson model. Springer, US, Boston, pp 208–209

Cruz-Piris L, Rivera D, Marsa-Maestre I, De la Hoz E, Velasco J (2018) Access control mechanism for IoT environments based on modelling communication procedures as resources. Sensors (Basel, Switzerland) 18:03

Dib O, Toumi K (2020) Decentralized identity systems: architecture, challenges, solutions and future directions. Ann Emerg Technol Comput 4(19–40):12

Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J 8(14):11717–11731

Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) iblock: an intelligent decentralised blockchain-based pandemic detection and assisting system. J Signal Process Syst 10:1939–8115

Ferdous MS, Poet R (2013) Dynamic identity federation using security assertion markup language (saml). Policies Res Identity Manag 131–146

Fernandez F, Alonso A, Marco L, Salvachua J (2017) A model to enable application-scoped access control as a service for IoT using oauth 2.0. In: 2017 20th conference on innovations in clouds, internet and networks (ICIN), pp 322–324

Ferrag MA, Maglaras L, Derhab A (2019) Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends. Secur Commun Netw 04

Ferraiolo DF, Barkley JF, Kuhn DR (1999) A role-based access control model and reference implementation within a corporate intranet. ACM Trans Inf Syst Secur 2:34–64

Fett D, Küsters R, Schmitz G (2016) A comprehensive formal security analysis of oauth 2.0. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, CCS '16, New York, NY, USA, Association for Computing Machinery, pp 1204–1215

Geepalla E, Bordbar B, Du X (2013) Spatio-temporal role based access control for physical access control systems, pp 39–42

Jia X, Hu N, Su S, Yin S, Zhao Y, Cheng X, Zhang C (2020) Irba:an identity-based cross-domain authentication scheme for the internet of things. Electronics 9(4)

Jindou J, Xiaofeng Q, Cheng C (2012) Access control method for web of things based on role and SNS. In: 2012 IEEE 12th International conference on computer and information technology, pp 316–321

Jin J, Shen M (2012) Analysis of security models based on multilevel security policy. In: 2012 international conference on management of e-commerce and e-government, pp 95–97

Kolter J, Schillinger R, Pernul G (2007) A privacy-enhanced attribute-based access control system. In: Barker S, Ahn G-J (eds) Data and applications security XXI, Berlin, Heidelberg. Springer, Berlin, pp 129–143

Lazouski A, Martinelli F, Mori P (2010) Usage control in computer security: a survey. Comput Sci Rev 4(2):81–99

Lee JY, Lin WC, Huang YH (A lightweight authentication protocol for internet of things. In: 2014 International symposium on next-generation electronics (ISNE), pp 1–2

Mahalle PN, . Prasad NR, Prasad R (2014) Threshold cryptography-based group authentication (TCGA) scheme for the internet of things (IoT). In: 2014 4th International conference on wireless communications, vehicular technology, information theory and aerospace electronic systems (VITAE), pp 1–5

Mahkonen H, Rinta-aho T, Kauppinen T, Sethi M, Kjällman J, Salmela P, Jokikyyny T (2013) Secure m2m cloud testbed. In: Proceedings of the 19th annual international conference on mobile computing &amp; networking, MobiCom '13, New York, NY, USA. Association for Computing Machiner, pp. 135–138

Ouaddah A, Elkalam A, Ouahman A (2017) Fairaccess: a new blockchain-based access control framework for the internet of things. Secur Commun Netw 9:02

Park J, Sandhu R (2004) The ucon<sub>abc</sub> usage control model. ACM Trans Inf Syst Secur 7:128–174

Pasquier IB, Ouahman AA, Kalam AAE, de Montfort MO (2015) Smartorbac security and privacy in the internet of things. In: 2015 IEEE/ACS 12th International conference of computer systems and applications (AICCSA), Los Alamitos, CA, USA, pp 1–8. IEEE Computer Society, Nov 2015

Pereira PP, Eliasson J, Delsing J (2014) An authentication and access control framework for COAP-based internet of things. In: IECON 2014—40th Annual conference of the IEEE Industrial Electronics Society, pp 5293–5299

Porwal S, Mittal S (2017) Implementation of ciphertext policy-attribute based encryption (cp-abe) for fine grained access control of university data. In: 2017 Tenth international conference on contemporary computing (IC3)

Recordon D, Reed D (2006) Openid 2.0: a platform for user-centric identity management. In Proceedings of the Second ACM Workshop on Digital Identity Management. DIM '06 (New York, NY, USA). Association for Computing Machinery, pp 11–16

Sandhu RS (1998) Role-based access control. Adv Comput 46:237–286

Sciancalepore S, Piro G, Caldarola D, Boggia G, Bianchi G (2017) Oauth-iot: an access control framework for the internet of things based on open standards. In: 2017 IEEE symposium on computers and communications (ISCC), pp 676–681

Smeets B (2019) Evolving SIM solutions for IoT. ericsson, 27 May 2019

Teravainen T (2020) What is single sign-on (sso) and how does it work? Apr 2020

Tomanek O, Kencl L (2016) Security and privacy of using ALLJoyn IoT framework at home and beyond. In: 2016 2nd International conference on intelligent green building and smart grid (IGBSG), pp 1–6

Xu R, Chen Y, Blasch E, Chen G (2018) A federated capability-based access control mechanism for internet of things (IoTs) 04:2018

Xu R, Chen Y, Blasch E, Chen G (2018) Blendcac: a blockchain-enabled decentralized capability-based access control for IoTs. In: 2018 IEEE International conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE Smart Data (SmartData), pp 1027–1034

Zhang G, Tian J (2010) An extended role based access control model for the Internet of Things. In: 2010 International conference on information, networking and automation (ICINA), vol 1, pp V1–319–V1–323

Zhao G, Si X, Wang J, Long X, Hu T (2011) A novel mutual authentication scheme for internet of things. In: Proceedings of 2011 International conference on modelling, identification and control, pp 563–566

Chapter 4
Lightweight Cryptographic Techniques and Protocols for IoT

Shubham Gupta and Sandeep Saxena

4.1 Introduction

In the academia and industry, Internet of Things (IoT) is achieving the highest importance and significance. The primary objective of the IoT is to connect the smart devices that can be installed in any framework for collaborating withother devices. This evolution could be possible in the authentication protocols, sensor devices, lightweight computing, and machine-type communication (MTC). As per the Deloitte report in 2021, IoT technologies are obtaining millions of investment from various research organizations to fulfill this vision (Deloitte 2021). Additionally, IoT technology is expected to play a vital role to improve the automobiles sector, health care, supply chain management, industrial applications, and smart cities. In this chapter, we attempt to present an outline of the existing IoT protocols and that are suggested for various layers such as logical link control (LLC), network, transport, and session layer. We discuss the standards presented by the Third Generation Partnership Project (3GPP), International Telecommunication Union (ITU), Institute of Electrical and Electronics Engineers (IEEE), and other standards organizations.

From early in 2004, various IEEE and ITU standardization committees started achieving the framework for the communication schemes of the IoT applications. The specification with the tallest extant contact is IEEE 802.15.4 (Marco et al. 2021), which specifies a small potential natural coat, and upon which the largest IoT machinery have constructed. It also establishes a medium access control (MAC), which is the basis for ZigBee 1.0 and ZigBee 2006 (Winter et al. 2012). It is possible that the MAC protocol's single-channel design form an ambiguity in the correctness, especially in multi-hop scenarios. This protocol, known as Time Synchronized Mesh Protocol (TSMP), became the industry standard for low-power wireless reliability

S. Gupta (✉)
Department of Computer Science and Engineering, SRM University,
Amravati, Andhra Pradesh 522502, India
e-mail: guptashubham396@gmail.com

S. Saxena
Director-IQAC and Professor-IT, IMS Unison University, Dehradun, Uttarakhand, India
e-mail: saxena.s.in@ieee.org

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_4

in industrial applications. The time-organized channel hopping was unified into the IEEE 802.15.4 standard from the IEEE 802.15.4e working band and will thus become a MAC protocol in the future revision of the IEEE 802.15.4 standard.

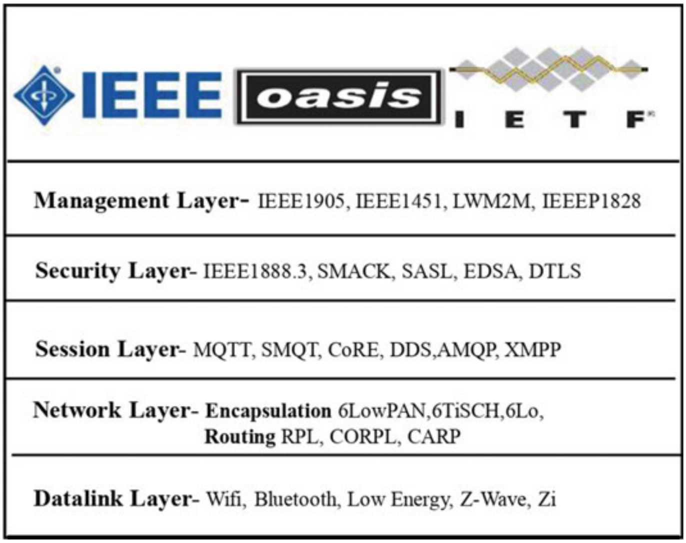
Several IETF working groups, including 6LoWPAN (Bhale et al. 2021) as a consolidation phase, ROLL RPL (Diniesh et al. 2021) as a routing protocol, and CoAP (Abhishek and Sanmeet 2020; Sowmya et al. 2021), help to integrate low-power wireless networks into the Internet. For years, low-power, dependable wireless multi-hop connections are becoming a real thing. For instance, Emerson is a method management behemoth1, claims to be have installed more than 9200 connections across every region, totalling more than 987 million operating times. Some networks use frequency tunnel revolving. There are a number of compact safety guidelines offered as a tool-constrained IoT smart gadgets. Although while using IoT network that was connect IoT gadgets to asset machine in cloud technology environments, these protocols may become security holes. Such systems are known as symmetric programming frameworks. A compact security method applied in symmetrical computing network that might provided required degree of safety to IoT components that function primarily outside companies' peripheral security. However, cloud such as asset platform that could manage tougher safety procedure operate heavily polluted web settings in which case compact procedures might pose a serious security risk.

Many businesses have highlighted the need of IoT security. According to the IoT standard architecture, IoT security consists of five functional components: identity management, authentication, authorization, key exchange and management, trust, and reputation. Apart from confidentiality, integrity, and availability, it also involves authentication, access control, and non-repudiation. All of these goals can be accomplished using cryptographic primitives. Cryptography can help to ensure the confidentiality and integrity of information. But traditional cryptography approaches, on the other hand, need a significant amount of resource allocation. IoT devices, on the other hand, are distinguished by restricted processing capacity, memory, power supply, and battery life. It is evaluated that several sensor nodes were utilized for the WSN and discovered that resource-constrained devices contain as little as 2 kilobytes (kB) of Random Access Memory (RAM). This clearly demonstrates the necessity for lightweight cryptographic (LWC) methods to be developed for information security. In addition, a detailed performance study was performed in terms of chip size, energy, and power, hardware and software efficiencies, and throughput latency.

The remainder of this chapter is structured as follows: The discussion on international bodies of IoT protocol development in Sect. 4.2. We also demonstrate the various protocols of IoT in Sect. 4.3. In Sect. 4.4, various IoT protocols and its features, characteristics are discussed. The lightweight cryptographic protocols with its techniques are illustrated in Sect. 4.5. Finally, Sect. 4.6 brings the article to a close.

4.2 International Bodies for IoT Protocol Development

Market, acquisition, interconnection, integration, analysis, applications, and services are all layers of the IoT framework. Smart grid, connected home, smart health, and so on are examples of market layers or application domains at the bottom layer. The second layer is made up of detectors and smart gadgets which serve as base of program. The class and allocation of sensors change according to the application. The third layer is the connectivity layer, which allows sensor data to be communicated to a data center or the cloud. Moreover, the consolidated information is investigated using machine learning and data mining method. Finally, the top layer is made up of resulting services as energy and health management, automation, industrial IoT, and so on. Each of these seven layers, which are stacked on top of each other, requires security and management. The data link layer is a layer that links two IoT devices, such as two devices or a device and a gateway sensor that links a group of devices to the web. Prior to connecting to the Internet, many sensors are frequently required to transmit and aggregate data. The session layer protocols allow various parts of the IoT communication subsystem to communicate with one another. Several standardization groups have suggested standards to cover all five levels. IEEE, IETF, and ITU are some of the most well-known. In general, IEEE focuses on data links, IETF on networks, and numerous institutions on session, privacy, security, and administration as shown in Fig. 4.1.


IEEE
oasis
I E T F

Management Layer- IEEE1905, IEEE1451, LWM2M, IEEEP1828

Security Layer- IEEE1888.3, SMACK, SASL, EDSA, DTLS

Session Layer- MQTT, SMQT, CoRE, DDS,AMQP, XMPP

Network Layer- Encapsulation 6LowPAN,6TiSCH,6Lo,
Routing RPL, CORPL, CARP

Datalink Layer- Wifi, Bluetooth, Low Energy, Z-Wave, Zi

Fig. 4.1 Layers and their related protocols

4.2.1 IoT Data Link Protocols

The data link layer protocol standards are discussed in this section. The topic covers physical (PHY) and MAC slab procedures, which are integrated maximum criteria.

4.2.1.1 IEEE 802.15.4e

IEEE 802.15.4 is an information connection protocol which is widely utilized in MAC coat. The norm defines the image form, crossbar, direction, origin of location, and the method through which links can communicate with one another. Traditional networking frame formats are incompatible with IoT devices with limited battery life. IEEE 802.15.4e was established in 2008 to expand IEEE 802.15.4 to include assistance for limited cooperation. It employs duration synchronization and networks floating to provide huge level of dependability and limited interaction in IoT data connections. The artist can create the scheduling algorithm depending on application demands; nevertheless, scheduling must fulfill mobility and handover criteria in order to be approved by guidelines. Planning could be integrated by a controller link, that is in charge of creating an agenda, notifying everybody about its additional connections, and simply following the agenda (Kinza et al. 2020).

Synchronization: Node synchronization is required to keep networks connected to the people around them and in addition to gateway. It is possible to do this using acceptance set or box-built synchronization. In endorsement option, networks that have previously established connection transmit for endorsement, stability assurances, which may also be utilized as sustain connections.

Network Formation: Advertisement of the network and requests to join are two critical needs for every MAC protocol. In 802.15.4e, nodes listen for advertisement orders and, if they receive at least one that could be delivered an invitation to join the advertising gadget. The join request in a centralized network is directed to manager node and handled there, but in a distributed system, it is processed locally. When a device joins the network and becomes fully functioning, the formation is deactivated and will be triggered again if another join request is received (Karalis et al. 2018).

4.2.1.2 Z-Wave

Z-Wave is a limited usage MAC norms that were originally intended home robotics and are now widely utilized in various IoT software, featuring smart homes and small business domains. It has a capacity of 30 m, to specific point connectivity, and suited for sending short notifications. That is employed CSMA/CA for communications links, as well as tiny ACK messages, to ensure reliable delivery. It has a mentor design where the mentor supervises servant, gives orders, and controls network organizing (Naidu and Kumar 2019).

4.2.1.3 ZigBee

ZigBee is a medium-range wireless communication protocol that is widely used in IoT. Smart homes, remote controls, and healthcare systems all rely on communication. Star, peer-to-peer, and cluster-tree are some of the networking topologies available. There are two stack profiles defined by the ZigBee standard: ZigBee and ZigBee Pro. These packet features provide complete overlap collaboration operate a variety of implementations. ZigBee Pro has additional appearance such as symmetric-key swap security, adaptability via erratic site appointment, and improved achievement via capable several transport techniques (Krejčí et al. 2017).

4.2.1.4 LTE-A

Long-term evolution advanced (LTE-A) is a set of modular connectivity norms developed to fulfill the needs of M2M and IoT networks. When compared to other cellular protocols, it is the best adaptable and profitable. It has traditionally depended on orthogonal frequency division multiple access (OFDMA) which is an intermediate approach method, splits the density into many bearer. LTE-A structure comprises the radio access network (RAN), core network (CN), and mobile nodes. The CN oversees managing mobile devices and keeping track of their IP addresses. The RAN is in charge of developing the command and information planes, as well as transmitter connection and transmitter control. RAN and CN interact through the S1 connection, with RAN consisting of eNBs to which additional mobile nodes are wirelessly linked. Furthermore, the latest LTE-A versions (LTE Rel-13 and Rel-14) provide new capabilities tailored to the forthcoming 5G needs (Limei et al. 2018).

4.2.1.5 DECT/ULE

Digital enhanced cordless telecommunications (DECT) is a cordless phone standard developed by the European Union. They have offered an addition called DECT/ULE that defines a less-power and minimum-cost air interface technology that may be utilized for IoT applications. It contains a committed channel chore and, as a result, is significantly more tolerant to interference and congestion problems (Jetmir et al. 2018; Salman and Jain 2019).

4.2.2 Network Layer Routing Protocols

In this part, we will go over several IoT routing standards and protocols in detail. It should be mentioned that the circuit stratum in the connectivity layer is divided into two instances in this paper: a routing layer that manages packet transmission from origin to terminal, and an encapsulating coat that creates wrapper.

4.2.2.1 RPL

The Routing Protocol for Low-Power and Lossy Networks (RPL) is a distance-vector protocol developed by the Internet Engineering Task Force (IETF) that uses into IoT systems. It enables all earlier mentioned MAC layer techniques, as well as a few more that aren't specifically developed for IoT. It was established on destination-oriented directed-acyclic graphs (DODAG), which have just one path from all leaf endpoint to the source, where everyone movement from the leaf endpoint is sent. Initially, every network broadcast a DODAG information object (DIO) identifying themselves as a core. DIO is spread above the connection, and the entire DODAG is progressively created. While conversing, structure delivers a destination advertisement object (DAO) to its parents, which is proliferated to the stem, who determines where to route it based on the destination. RPL links can be either orphaned (the highest popular) or stateful. An orphaned network simply maintains monitor of its parents. Only origin has a comprehensive understanding of the DODAG. As a result, all correspondence pass via shell (Kim et al. 2017).

4.2.2.2 CARP and E-CARP

Another routing technique based on dispersed networks and developed for underwater communication is channel-aware routing protocol (CARP). It is a lightweight packet forwarding technology that may therefore be used in IoT devices. It chooses the forwarding path based on past connection quality evaluations. The two eventualities that such protocols should take into account are network startup and data forwarding. A HELLO box is transmitted from the plunge to always different links in the network during network setup. The primary issue such as CARP is it does not enable to reuse of earlier acquired information. Instead of, utilization only needs device information when it switches considerably, CARP data transmission isn't useful for that application. In E-CARP, the sink node was given the ability to store previously received sensory input, which improved CARP. When fresh information was required, E-CARP transmits a ping bag, to which the sensor nodes respond with new data (Sharma et al. 2020).

4.2.2.3 6LoWPAN

IPv6 over low-power wireless personal area network (6LoWPAN) was among the earliest and most widely utilized IETF protocols in this class. It effectively wraps IPv6 lengthy crossbar in IEEE802.15.4 tiny MAC packets with a maximum length of 128 bytes. Many characteristics are supported by 6LoWPAN standards, including varied address lengths, diverse Internet fundamentals, low Internet, minimal power usage, cost-effective, accessible connection, mobility, dependability, and extended sleep periods. Header reduction is employed in the norms to decrease transmitter overpass, dissolution to satisfy the 128-byte highest border width in IEEE802.15.4, and support for multi-hop delivery. Any frame that does not comply with the 6loWPAN standards is rejected in the No 6loWPAN header scenario. Fragmentation headers are used to split lengthy IPv6 headers into 128-byte pieces, whereas mesh headers are used for broadcasting (Sharma et al. 2020).

4.2.3 Session Layer Protocols

In this part, we look at a number of IoT activity stack procedures that are utilized for directive transmission and have been standardized by various standards bodies. TCP and UDP are the main protocols at the transport layer for the majority of applications, including IoT. However, depending on the IoT application needs, multiple message delivery functions are necessary. It is preferable that these functionalities be implemented in standard, compatible methods.

4.2.3.1 MQTT

Message queue telemetry transport (MQTT) is designed by the Organization for the Advancement of Structured Information Standards (OASIS). This is a publish/subscribe architecture in which the system is divided into three parts: publishers, subscribers, and a broker. Publishers on the Internet of things are small sensors that connect to a broker to provide data and then go back to sleep as soon as feasible. Members are registered that is keen in particular topics, such as sensitive information, and link to brokers to be notified when additional information is delivered. The brokers categorize tactile input into categories and deliver it to followers who are solely interested in unique areas (Kalyani and Chaudhari 2020).

4.2.3.2 AMQP

Advanced Message Queuing Protocol (AMQP) is an OASIS conventional for the financial region that operates above TCP and employs share/subscribe structure identical to MQTT. The most significant distinction between both standards is that the trader is split into two parts: interchange and lines. The interchange component is in charge of receiving reporter comments and routing them into chain and created on predefined characters. Members connect to such lines, which essentially indicate the subjects, and obtain sensual input as soon as it becomes available (Soni and Makwana 2017).

4.2.3.3 XMPP

The Extensible Messaging and Presence Protocol (XMPP) was initially intended for chat and message sharing function. It is created on the XML language and was standardized by the IETF over a century now. It is widely utilized and extremely effective when utilized via web. Its use has recently been expanded for IoT and SDN applicants because of standardized uses of XML, which provides it simply extendable. It does not give any excellent services assurances and, as a result, is unsuitable for M2M connections. Furthermore, because of the numerous headers and tag formats, XML messages generate additional overhead, increasing power consumption, which is essential for IoT applications (Kanakaris and Papakostas 2020).

4.2.3.4 DDS

The Object Management Group created the Data Distribution Service (DDS) as a communications standard (OMG). It has a share/register structure and is primarily used for M2M connections (Raposo et al. 2018). The most advantageous aspect of this procedure is the high value of function tiers dependability provided by the use of a broker-less structure, which is ideal for IoT and M2M connections. The publisher layer is in charge of sensory data transmission. Data writers collaborate with editors to agree on the facts and updates that will be provided to subscribers. Viewers are the recipients of physical facts sent to the IoT request. Publishers receive featured facts and distribute it to subscribers, while subjects are the many sorts of data that are released (Zhang 2018).

4.2.4 IoT Management Protocols

This paragraph provides summary of different management procedures utilized in IoT to manage and communicate weird devices. We begin by describing two strategies for dealing with facts connections duality. Then, we will go through several controller gadget management procedures that are commonly utilized in M2M and IoT solutions. Due to the diversity and requirements at different tiers of networking, management protocols play a key role in IoT. For IoT applications, diverse and simple collaboration around procedures at the similar or identical levels is important.

4.2.4.1 IEEE 1905.1

IoT includes a wide range of MAC layer procedures; hence, compatibility across these norms is important. This IEEE norms would manage unity by offering an abstraction thickness that sits on peak of everyone of these disparate MAC procedures. This abstraction conceals the variety of distinct procedures, allowing them to communicate without needing any changes to their layout. The abstraction thickness enables the transmission of comments known as control message data units (CMDUs) across every norms-compliant devices (Savvidina Auliva et al. 2018).

4.2.4.2 LWM2M

Other OMA procedure that is especially developed for IoT machines management is lightweight M2M. It is a client–server protocol that uses JASON messages (JavaScript Object Notation). It is primarily based on CoAP, although it may also be used with other activity procedure. This procedure is utilized to control machine operations via the connection, transport facts from the connection to machines, and is extensible to numerous IoT connection client communications (Khusanbek and Tai-Myoung 2019).

4.2.5 Security of IoT Protocols

Another difficulty to address at all networking tiers described in the preceding sections is providing security for IoT platforms. Due to their complexity and resource consumption, traditional security techniques such as encryption and public-key infrastructure appear unfeasible for IoT devices. As a result, new standards for lightweight security architectures are being created.

4.2.5.1 TLS/DTLS

Two frequently used security protocols are transport layer security (TLS) and datagram TLS (DTLS). They primarily offer authentication, integrity, and secrecy at the transport layer and are commonly employed in CoAP protocols. They primarily offer authentication, integrity, and secrecy at the transport layer and are commonly employed in CoAP protocols. TLS and DTLS are made up of two compartments of procedures, record, and handshaking, that handle encapsulation and identification, accordingly. Traditional security techniques can be used to provide credentials, signatures, and error handling in these standards, but they have been changed to meet resource-restricted devices used in IoT (Mavromatis et al. 2019).

4.2.5.2 SASL

Simple authentication and security layer (SASL) is additional IETF protection architecture for providing identification in IoT registration via networks. It separates the proposal from the identification method and authenticates clients using application-specific authentication techniques utilizing simple messages. In IoT, this architecture is often enabled by session layer protocols that accept TLS and SSL, such as MQTT and AMQP (Urien 2017; Coppolino 2019).

4.2.6 IETF on IoT Security

Despite the numerous security methods and standards developed for IoT, threats and malicious conduct remain issues that necessitate more innovation. Many of those problems and safety needs are addressed in many current IETF proposals, which we will outline below. Various IoT security concerns and requirements are described in (Nastase 2017; Hannes and Emmanuel 2019). The lifecycle of IoT devices is discussed, as well as mechanisms for providing security during the device's upgrading, procedure, changes, and end-of-life steps. They present various IoT characteristics, or use instances and talk the safety procedures that are available for such features at various levels of the machine reproduction. The topic covers IoT safety needs, the usage of safety procedure to meet those needs, and the problems associated with employing such protocols. Furthermore, it is recommended for security solutions as well as implementation instructions that are beneficial to IoT companies. As a result, this chapter can be used as a standard for IoT safety baseline standards and existing safety concerns to be addressed in the future study.

4.3 Various Protocols for IoT

An overview of IoT protocols such as Bluetooth Low Energy, Thread, WirelessHART, Z-Wave, ZigBee, and the IP-Smart is provided. The stacks of these protocols were picked after researching stacks primarily designed for various use-cases and because they are thought to be protocol stacks that have maintained themselves in the current scenario. IP-Smart is a recommended protocol stack established on IEEE- and IETF-defined protocols that have the chance to interfere in all use-cases while not limiting device accessibility through the use of proprietary protocols or techniques.

4.3.1 ZigBee

The ZigBee alliance is made up of 450 participants from technology firms, colleges, and government organizations who work together to establish and promote IoT protocols. The objective is to create dependable and simple guidelines for usage in domestic, business, and corporate applications such as smart houses, health care, and smart grid, among others. ZigBee's protocol suite is based on the widely-known broadband specification 802.15.4 and includes its own network interface as well as an online portal surface for particular ZigBee or OEM programs. ZigBee 3.0 is the current trend that unifies the preceding different network norms: ZigBee Pro, ZigBee RF4CE, and ZigBee IP/920IP. A ZigBee network utilizes a grid architecture to enable identity among communications systems, avoiding the connection from having a central point of failure (Gupta and Singh 2020). ZigBee systems are adaptable enough to handle existing affiliates with more than 350 locations, and the network is made up of three separate component types: coordinator, router, and end device.

In order to accomplish secure communication, the connecting machine and the Security Unit generate a 16-octet unique challenge (Datta and Sharma 2017) and send it to everyone to compute a response. ZigBee IP provides complete IP cellular network for ZigBee and includes TLS1.2, allowing TLS Handshake for identification. For data transmission, ZigBee employs the SKKE mechanism (Symmetric-key Key Establishment). It creates a connection between both the network hub as well as the Trust Center using a Link Key. Prior research has shown that when ZigBee is utilized at the Specification Access Control, the symmetric encryption protocols are susceptible to sniffer attacks. Whenever gadgets wish to join the connection, the Security Hub will broadcast the network key unprotected over-the-air, and capturing this key might provide the hacker the ability to access information in the system and execute spoofing.

Inside the ZigBee network, devices offer a Security Hub that is important because of the following transmission, end-to-end application service management, uninstalling items from the system, maintaining the device list, and maintaining the authorization customization database. Whether a gadget is well before as a Security Hub determines which gadget needs to take on the function of Network Gateway. In this situation, all equipment connect to the network must be well before with the Primary Keys location and first verification code. If the Security Hub is not well before, it switches to the ZigBee Coordinator or a router specified by the ZigBee Coordinator. To maintain data security, ZigBee employs a System Key for encryption network frames with AES 128-CCM (Marksteiner et al. 2017). It is an unique code accessed by all connected devices, and an alternative session key is created at specific phases to succeed the existing key and offer key cycle. Device management is performed by the Administrator and/or Authentication Server and includes responsibilities such as updating device listings and removing devices from the system if they do not meet the system security that has been specified.

4.3.2 Thread

Thread organization has been floated by Google Nest Labs as a trade association comprised of many top global companies to build and collaborate on a new norm to deliver a user-friendly, safe, accessible, and capacitor control plane for each and every wired headset. The physical layer is based on well-known and proven techniques such as 802.15.4, 6LoWPAN, and UDP, and it has specified its physical layer. A Thread system is composed of various device kinds. A Routing Protocol is a router that acts as the interface between the 802.15.4 network and neighboring networks that use various physical layers, such as 802.11. Establishing a loop system needs at least one barrier routers, but additional can be added as needed (Cline 2017).

In addition to portal capabilities, the routing protocol provides routing services for off-network operations. Routers offer sensor nodes with navigation, connecting, and security functions. They are intended to always be on, although they can be reduced to the Router-eligible End Devices (REED). It serves as secondary components in system and is engaged as firewalls when required, with no user input required. Thread connections will auto-initialize as cellular networks. Mesh Link Establishment (MLE) messages create and set up safe wireless connections, identify neighbor gadgets, and keep transportation expenses between devices in check. In order to provide data security for the Thread channel, a series of participants must be created. When a machine desires to connect to the network, it initiates a DTLS handshake with the controller in order to validate itself. The regulator is a cellular modem, such as a smartphone, that communicates with both the connecting device directly via the network gateway. The DTLS connection provides device identification as well as the safe transmission of information security settings. Aside from that, Thread works as a peer connection, with all machines communicating the very same data, and if designated as REED, may act as a controller and commissioner in the channel as necessary. The Thread network employs a Provider Passcode to secure 802.15.4 MAC transmitted data against spying or deliberate interruption. The Ethernet Code is stated (Afzal et al. 2019) to be identifier of the HMAC 32-bit key utilizing a key card, with no knowledge of the primary/master key computation.

4.3.3 Bluetooth Low Energy (BLE)

BLE was incorporated in Bluetooth 4.0 standard (Terán et al. 2017). It has been created to bring Bluetooth connectivity to the low-powered interfaces, as well as to make it easier to integrate with portable smart phones and tablets. This method varies from the existing IoT physical layer in that it provides the out-of-the-box capability for interaction with portable devices, rather than requiring a perimeter network, as Thread and ZigBee do. Simply works will authorize any device that sends a connection request, but Passkey requires process information to authorize a receiver. With the inclusion of BLE secure links in the standard protocol of Bluetooth 4.2 (Ensworth and Reynolds 2017), BLE may employ ECDH for data transmission. BLE transmitters based on prior Bluetooth versions (4.1 and before) use their own Key Routing Protocols for data transmission. Depending on the manner of launching, the program decides on a TK (Temporary Key) and generates the Short TK (STK) that generates the Long TK (LTK). If the BLE symmetric encryption does not use ECDH encryption, it is vulnerable to monitoring (Zhang et al. 2020). BLE uses an Identity Resolving Key (IRK) to convert confidential to global machine location conversion, which helps gadgets avoid being traced by their stable web network. A Connection Signature Resolving Key (CSRK) is used to facilitate information authentication in order to safeguard a link between two machines.

4.3.4 WirelessHART

The WirelessHART control plane has been linked to the proposed system, as illustrated in the image. In a WirelessHART system, the portal functions as the entry point, system administrator, server admin, portal, and HOST functionality. A entry point is the wireless network required for network management, commissioning new products, and interacting with the wired HART interface (Adriano et al. 2018). A WirelessHART system comprises entry points/router equipment, as well as field devices, in addition to the portal. It may be scaled up to tens of thousands of devices if required by including several portals into the network. There isn't much data given about how WirelessHART handles authentication scheme. All evidence shows that the Join Id is used to validate the Network Protocol Data Unit (NPDU) payload and confirm a Message Integrity Code (MIC) of the entering approach, and that it is used to validate the NPDU contents and check a Message Integrity Code (MIC) of the entering notification. WirelessHART may employ 802.15.4 to construct an Access Control List. According to WirelessHART (Raposo et al. 2018) technical notes and network guidelines, the entry point should have a privacy policy that describes various user profiles with varying access to vital safety and customization settings. Suppliers appear to be in charge of implementing these security procedures, indicating that suppliers must offer enough protection for user profiles to prevent illegal remote access. WirelessHART has integrated a session key and a data channel to ensure information secrecy. A system password encrypts and protects data coming from external hackers, whereas a key pair protects the network link between transmitter and receiver.

4.3.5 IP-Smart

The IP-Smart is a network architecture constructed from IETF and IEEE defined mechanisms, as well as prior work on a standardized protocol stack for the Internet of things. IEEE and IETF have suggested various conventional techniques, including 802.15.4 to link IoT-constrained equipment. A protocol stack of this type would provide IP technology to limited devices while being based on public, excellent norms. IP-Smart is thought to be capable of competing with the prior theoretical protocol suite while not being constrained by open-source communication protocols in the pursuit of fully integrated IoT devices. The IP-Smart network layer would provide a star or blend configuration for operating systems if 802.15.4 was used. The 2.4GHz band provides 16 broadcasters and rates up to 300 kbits/s with a scope of 15–35m. A machine can be classified as either a Full-function/Reduced-function Device (FFD/RFD). If a machine is a comprehensive item, it can work as the program's relay node. It will be in charge of maintaining data traffic and transmitting packet data, among other things. RFDs are unable to take on the responsibility of central controller and can only communicate with the normal node in a simple manner.

TLS or DTLS greetings can be provided via the IP-Smart protocol stack when using CoAP or MQTT. One of the most difficult elements of the IP-Smart application layer is key exchange. Recent work on 802.15.4 reveals issues such as no provision for cooperative keying, a system sharing key issue in replaying security, and insufficient support for pairwise keying. Current research on this topic has shown improvement, and ECDH has been applied. In the planned IP-Smart, 802.15.4 is incorporate an Access Control List (ACL) (Rajashree et al. 2018) including location, security suite, and vital information. Connectivity passcode prototype might be utilized to offer security mechanisms in the IP-Smart protocol layer.

4.4 Protocols and Its Features

We stress that one of the most important issues in IoT applications is privacy. As an outcome, many rules, prototypes, and research projects have been presented. Even though there are certain security measures inside IoT protocols, they are insufficient to properly safeguard IoT devices. We examine the cryptographic methods and interface specifications which are advocated for usage by IoT devices. We further looked through the most advanced National Institute of Standards and Technology (NIST) suggestions.

4.4.1 Cryptographic Techniques and Features

Cryptographic techniques are necessary to safeguard IoT devices static and in motion. These approaches meet various security needs, including privacy, data quality, entity identification, data encryption, key distribution, non-repudiation, reliable data platforms, and user authentication as shown in Fig. 4.2. Das et al. (Das et al. 2018) already offered a broad classification of multiple security procedures required for the IoT system in their earlier stuff. Their classification covered a variety of critical security forces like data security, human and device authentication, permissions, encryption techniques, and information security. They also provided a clear comparison of recently suggested IoT-related security measures for key security and operational characteristics. Moreover, they explored different security issues that must be handled in the future to enhance IoT security.

4.4.1.1 Encryption Protocols

This section goes through parts of the IoT ecosystem where cryptography protocols and standards are used.

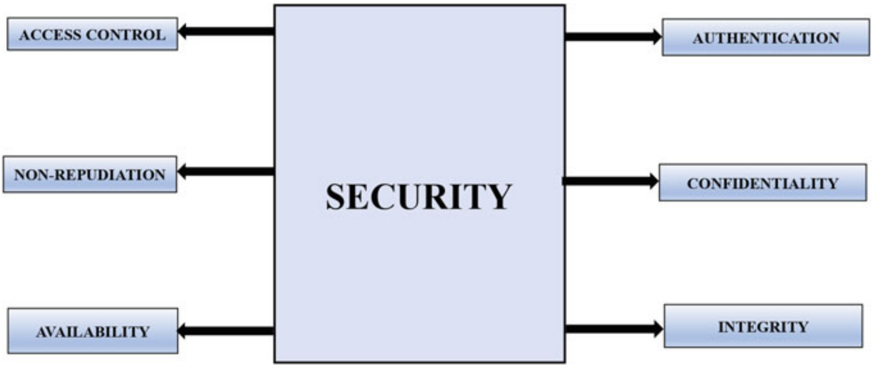


Fig. 4.2 Security needs and important features

- *Wearables security:* Wearable medical gadgets serve crucial role in health care. Telecommunications across smart technology and between them and databases may be vulnerable to a variety of malware activity, compromising the security and privacy of patient health information. Due to the resource constraints of portable tech, modern cryptography approaches that are being utilized to offer security for sensors including SHA and AES.
- *Device security:* TLS, PKE, and WPA2 are several cryptographic technology specifications used for IoT data security.
- *Network security:* The information security guidelines reflect different security requirements, as well as advice on procedures and techniques to perform multiple tasks, like safe administration and operation. There are many information security protocols for various kinds of devices that are suitable to IoT devices.

  Some of the information security requirements that apply to IoT systems are as follows:

1. 3GPP LTE is a high-speed wireless transmission platform for wireless smart phones. It offers a variety of intelligence community, like access privileges to IoT systems, secure transfer of signaling data and user information, and safe access to digital platforms, which includes authentication process via USIM and UE. LTE employs security protocols such as Cipher-based MAC and AES.
2. The Bluetooth connectivity platform facilitates the transmission of data between stationary and mobile IoT devices via narrow interaction. Identification, secrecy, authorization, and integrity verification are among the initial privacy services offered by the Bluetooth standard. The Bluetooth access control system employs a contest technique. The claimant or the validator is a machine that participates in the verification process. The claimant tries to prove its identification, while the validator confirms the claimant's authenticity. The challenge-response technique allows machines to confirm each other by validating understanding of a private key known as the Bluetooth connection key.

3. ZigBee 3.0 is based on the IEEE 802.15.4 standard requirements, which provide a worldwide frequency range of 2.4 GHz. IoT elements from various IoT platforms can interact with one another using the ZigBee 3.0 standard. Access control policy, login authentication of data, and image counter are among the security mechanisms provided by ZigBee networks. Using an access control policy, only machines that have previously been determined can participate in the channel. As a result, security precautions are implemented to prevent infiltration from potential enemy actors as well as nearby ZigBee systems. The 128-bit AES-based authentication is utilized for wireless networks to protect external factors from understanding ZigBee data packets.

- *Cloud security:* Due to purposes of privacy, it is important to safeguard data stored in the cloud. The information is recorded on a web server in cloud applications. As a result, a subscriber has no control over the information that has been saved. There seems to be a risk to information security, whether it is an outside or web attacker. From the standpoint of cloud providers, it is critical to ensure the accessibility of data that is directly related to business contentedness (Coppolino et al. 2017). SSL and Ip Network Protection are two encryption technique principles that are used to safeguard cloud data (IPSec).

Following that, we will cover the famous cryptographic algorithm guidelines that safeguard the information secrecy.

Symmetric and asymmetric cryptographic schemes: AES is assumed the required frame cipher for the wireless technologies to maintain security over cellular connections, and execute in transport layer security (TLS) framework. Public-key encryption techniques are also widely accessible. The IETF created numerous symmetric encryption specifications, like RSA and Elliptic Curve Cryptography (ECC) for web applications like Online Bulletin Access Point. The IEEE advisory committee also released many public-key encryption specifications, including general public cryptographic methods, and identity-based encryption algorithms utilizing couplings.

Encryption protocol standards for resource-constrained devices: IoT applications are frequently resource-constrained in different IoT contexts like wireless communication and smart grids, and they generally interact using wireless communication protocols such as ZigBee and Bluetooth. A complex encryption protocol employs just a few cryptographic functions, as well as security mechanisms of minimal length, to decrease computing and communication expenses for IoT devices. Due to the extreme low resources available on such machines, lightweight encryption standards are required.

4.4.1.2 Digital Signatures

A authentication ensures that the message was authenticated by the asserted signer and that it is not edited after the sign was produced by the signer's secret key. A validator that obtains signer's key pair may verify the signer's identity. Digital signatures are often employed in a variety of techniques, including Connected Vehicle Systems (CVS) and cryptographic-enabled protocols. Check out the following group evaluation scenario in IoT. Because of the limited resources of IoT systems, authenticating each message delivered in an IoT context becomes a difficult process. As a result, every digital signature authentication limits the effectiveness of the actual IoT network. In comparison, if the signatures are confirmed in groups, the validation time is significantly reduced. In IoT, RSA with PKCS is utilized for cluster authentication. For group validation in IoT, the compact ESDSA (Don et al. 2001) is chosen since RSA with PKCS is costly for low-power IoT devices. Additionally, we evaluate IoT protocol standards and examine their economic effect in terms of industrial IoT device implementation. We additionally point out a few of the protocols' shortcomings, including the necessity for software patches to correct security issues, identifying virus in programs, and the need for upgrades and/or new guidelines to manage IoT devices with the potential for optional links. NIST looked at the influence of encryption network protocols on corporate IoT equipment and found numerous concerns:

1. *Cryptographic mechanisms:* The AES protocol has a significant scope as follows. Let us consider, it is used in the verification and analysis of hundreds of industrial IoT devices. Moreover, newly accepted RFID protocols and lightweight security protocols have no or just one commercialized version that defines the fundamental characteristics of RFID for usage in the distribution network.
2. *System security engineering:* So far, it is unclear if network security experts use systems development techniques while designing and implementing IoT devices.

NIST has also indicated a number of standardized domains where additional effort is made in the future to enhance IoT security:

1. *Cryptographic techniques*: A cryptographic hash of the preceding block, as well as a collection by the sensor data, is included in every square of a database. It is becoming more popular in a variety of applications, including identity management systems (Jacobovitz 2016). For IoT security measures, upcoming data encryption norms must look at blockchain technology. The connected home processor is in charge of handling all input and output activities to and from the connected home from a centralized location. The miner may be integrated with the house's network interface, which would be used to connect IoT systems to the home network. Aside from the miner's security responsibilities, like payment validation, authorization, and monitoring, the miner can also do other tasks including spreading and upgrading passwords, altering transaction structure, and creating and maintaining the network.
2. *Network security*: In order to tackle IoT systems that establish impulsive links with no understanding of the complete system, modern laws must be updated and/or new rules must be established.
3. *System security engineering*: We must determine whether or not the general network security engineering principles can be used for IoT network.

4.5 Lightweight Cryptographic Techniques

IoT has made use of cryptographic techniques and interfaces like identity-based encryption (IBE), RSA, ECC, and so on. RSA is used to encode and transmit encoded symmetric keys for use with asymmetric algorithms. ECC is often used to protect communication between IoT devices by authenticating and agreeing on keys. Likewise, IBE (Dingding et al. 2020) facilitates certificate administration in IoT network by allowing a transmitter to encode a signal to the identification without having to obtain the public-key credentials. Also, ABE has been adapted to be acceptable for IoT devices by employing a gateway (Lihua et al. 2019). To ensure secrecy in IoT, these fundamental cryptographic methods are either changed or utilized in conjunction with other techniques or methods, as will be explained more below. Ensuring data security at restricted devices and during IoT connectivity is a critical challenge.

The asymmetrical capacities and low-power characteristics of the IoT provide challenges in obtaining this by the conventional cryptography methods outlined below. The lightweight cryptography system has two sub-approaches: i) key encryption: which encodes the current term password only at a time, ii) data encryption: which encodes numerous messages using similar data packet. This method delivers secrecy functions to devices and applications while incurring no additional processing or transmission overheads. To accomplish dynamic public-key management, the domain-specific IBE technique is utilized. Canteaut et al. (Canteaut et al. 2017) looked at symmetric primitives to see whether they could perform effectively on the web by utilizing fully HE (FHE) and transciphering to secure these savages. Following that, we will look at particular ECC, MANET, and WSN convergence strategies,

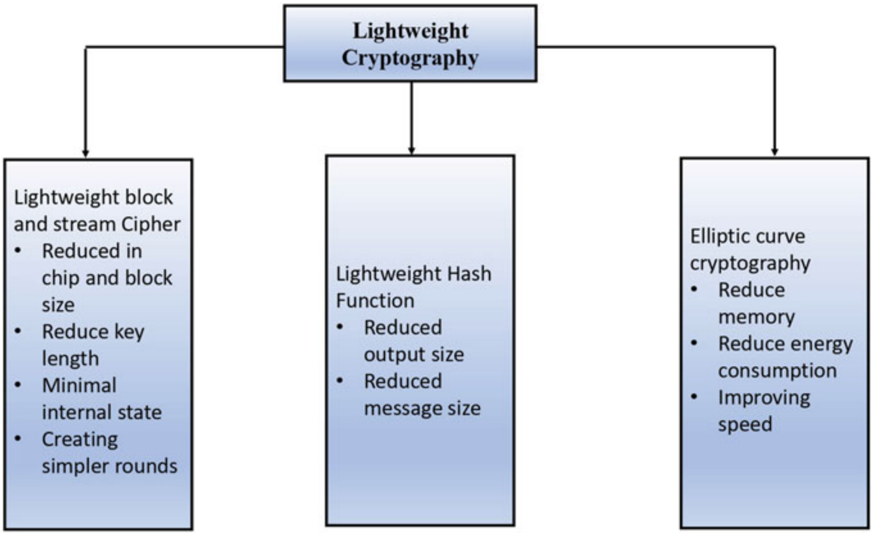

Lightweight Cryptography
Lightweight block and stream Cipher
• Reduced in chip and block size
• Reduce key length
• Minimal internal state
• Creating simpler rounds
Lightweight Hash Function
• Reduced output size
• Reduced message size
Elliptic curve cryptography
• Reduce memory
• Reduce energy consumption
• Improving speed

Fig. 4.3 Various cryptographic techniques for lightweight protocols

as well as dispersed and unloading techniques, header reduction, and cryptographic transformation methodologies for IoT as shown in Fig. 4.3.

1. *ECC-Based Algorithms*: The ECC-based methods are thought to be far competent and safe than traditional approaches since their credentials are shorter and provide the same layer of assurance. Here, we will go through several lightweight methods for IoT machine based on ECC. Despite utilizing the bilinear matching in the ABE scheme, an elliptic curve decisional DH (ECDDH)-based ABE system addresses data security and privacy in IoT smart devices. ABE-based bilinear pairing schemes feature modular exponentiation comparable to RSA, while 160-bit ECC gives privacy comparable to 1028-bit RSA. Yao et al. (Xuanxia et al. 2015) minimized transmission and computational overheads but operates badly in abolishing characteristics and adaptability for enabling a significant proportion of a program. This technique is not appropriate for IoT-constrained equipment while using multiattributes for ensuring privacy based on a linear relationship between computational and communication overheads.
2. *MANET and WSN to IoT*: MANETs and WSNs have equivalent available resources to IoT systems, enabling for the use of lightweight encryption methods in IoT. WSN and MANET are crucial components of IoT development and are important instruments for IoT systems. WSNs are small, lesser, and inexpensive equipment with sensors that gather information from the environment and other locations, whereas MANETs transfer that information to the server and other platforms without the need of present communication channels. WSN's reduced, resource-constrained autonomous devices are challenging to monitor, maintain, and defend from assaults. Baskar et al. (Baskar et al. 2016) improved results in terms of space and capacity by including chaotic map-based data encryption into the extended tiny encryption algorithm (XTEA). Furthermore, their system is not extensible to large data flow operations, making it a poor option for limited machine. The dispersed characteristic of the MANET is exploited by Kumar et al. (Chaitanya et al. 2018) to develop a compact encrypted communication method. Due to resource constraints and equipment portability, secure communication in WSN is difficult, but public-key encryption offers access policy and user authentication required for identification.
3. *Distributed and Offloading Methods*: Spread and unloading methods enable IoT embedded systems to spread or transfer encrypted processing to network elements. These methods help IoT systems in terms of processing and performance. Outsourcing enables source of energy equipment to use surrounding equipment, such as fog, edge, or cloud, to compute techniques such as ABE which is the computationally intensive. Furthermore, the broadcasting cryptographic technique (Blundo and Cresti 1994) enables a transmitter (messenger) to encode and transmit the encrypted message to a group of receivers, with only non-revoked listeners (receivers) being able to unlock it. Identity-based broadcast encryption (IBBE) methods were developed in which the identified traits of the transmitters are utilized as the public key to eliminate the need for certificate maintenance. The lightweight distributed access control system with search engine (LDAC-KS)

(Yang et al. 2017) resolves challenges connected to the safety of decentralized data processing of e-health records (EHRs). The sensor component gathers and secures patient medical records using the access policy, allowing each entity with a comparable characteristic to access the medical records.

This approach purports to raise the problem of resource-constrained e-health systems. However, this method only handles user-server communication and does not take into account fundamental general health equipment like body sensing equipment. Also, a semi-trusted method is designed for intensive computation during the data security stage, providing access of records while breaking privacy. Semi-static encrypted data allows the receiver to select an arbitrary figure of users at the time of authentication, increasing the ciphertext proportion of receivers' secret information. Using a general modification with bilinear projection and the decisional bilinear DH exponent (DBHE), the length of secret key and ciphertext are both cut by half.

4. *Header Compression Mechanisms*: For connection, IoT smart devices often employ conventional communication systems that are IP and IPv6 compatible via limited wireless personal area networks (6LoWPAN). Standardization enables researchers to enhance current interfaces for smart devices by utilizing packet header compression techniques. WSN connects the physical and digital worlds by using the unique features of actual devices connected to the Internet and the use of conventional TCP/IP interfaces to overcome device diversity and asymmetrical transmission security concerns. To overcome these problems, IP-based security measures, communication encryption, and dynamic load methods are commonly utilized. Glissa and Meddeb (Ghada and Aref 2019) suggested the IPsec-based security mechanism version at Contiki OS adaption surface. The 6LowPSec sensor utilizes current IEEE 802.15.4 hardware encryption capabilities and grid topology for lower end of the market communication between devices at the adaption phase. Despite the availability of threats, it generates new information and credentials for each phase to ensure secrecy, consistency, and authenticity. For asset IoT nodes, header reduction of network protocols frames dramatically reduces reaction time and resources usage. A variety of portable cryptographic systems were examined in this section, with information about each construction, benefits, and disadvantages given. Several techniques were classified as others that used ECC, MANETs, and WSN convergence, dispersed unloading techniques, header compression, and encrypted transformation technique.

4.6 Conclusion

In this chapter, we have presented a detailed overview of IoT applications. Most of these standards have been created and standardized by organizations such as the IETF, IEEE, ITU, and others, and many others are currently in the works. Moreover, we examined IoT management systems quickly and addressed a few of the current security measures and services offered at various levels of standardization.

We offered to provide a method of standardizing upcoming IoT systems. There are numerous protocols looking to maintain themself in the IoT industry, within each suggested answer to IoT needs. ZigBee, Z-Wave, and WirelessHART have been introduced to examine the various methods and how they compare in level of safety and suitability for application in various use-case sectors. Specifications that provide their own procedures to allow various security functions have been found to have vulnerabilities when compared to utilizing more developed and acknowledged assistance. Additionally, we describe IoT electronic objects that can support traditional cryptographic techniques. In this scenario, a newly ultralight cryptographic fundamental that delivers equivalent or more safety than traditional savages may be a preferable option. Furthermore, numerous IoT smart devices are still resource-constrained, and an examination of the various ultralight cryptography algorithms verifies the relevance of our subject.

References

Abhishek K, Sanmeet K (2020) Internet of things (iot), applications and challenges: a comprehensive review. Wireless Personal Commun 114:1687–1762

Adriano JD, Carlos do Rosario E, Rodrigues JJPC (2018) Wireless sensor networks in industry 4.0: Wirelesshart and isa100. 11a. In: 2018 13th IEEE International conference on industry applications (INDUSCON), pp 924–929. IEEE

Afzal B, Umair M, Asadullah Shah G, Ahmed E (2019) Enabling iot platforms for social iot applications: vision, feature mapping, and challenges. Fut Gener Comput Syst 92:718–731

Baskar C, Balasubramaniyan C, Manivannan D (2016) Establishment of light weight cryptography for resource constraint environment using fpga. Procedia Comput Sci 78:165–171

Bhale P, Biswas S, Nandi S (2021) Liene: lifetime enhancement for 6lowpan network using clustering approach use case: smart agriculture

Blundo C, Cresti A (1994) Space requirements for broadcast encryption. In: Workshop on the theory and application of of cryptographic techniques, pp 287–298. Springer

Canteaut A, Carpov S, Fontaine C, Fournier J, Lac B, Naya-Plasencia M, Sirdey R, Tria A (2017) End-to-end data security for iot: from a cloud of encryptions to encryption in the cloud. In: Cesar Conference

Chaitanya Kumar N, Basit A, Singh P, Venkaiah VC (2018) Lightweight cryptography for distributed pki based manets. arXiv e-prints, arXiv–1804

Cline G (2017) Product development in the era of iot: tying the digital thread. In: Aberdeen Group

Coppolino L, DAntonio S, Mazzeo G, Romano L, (2017) Emerging threats and current solutions. Cloud security. Comput Electr Eng 59:126–140

Coppolino L, D'Antonio S, Mazzeo G, Romano L (2019) A comprehensive survey of hardware-assisted security: from the edge to the cloud. Internet of Things 6:100055

Das AK, Zeadally S, He D (2018) Taxonomy and analysis of security protocols for internet of things. Future Gener Comput Syst 89:110–125

Datta P, Sharma B (2017) A survey on iot architectures, protocols, security and smart city based applications. In: 2017 8th International conference on computing, communication and networking technologies (ICCCNT), pp 1–5. IEEE

Deloitte (2021) Internet of things (iot): the rise of the connected world, pp 1–34

Dingding J, Yamin L, Bao L (2020) Ibe with tight security against selective opening and chosen-ciphertext attacks. Designs Codes Cryptogr 88(7):1371–1400

Diniesh VC, Murugesan G, Joseph Auxilius Jude M, Harshini A, Bhavataarani S, Gokul Krishnan R (2021) Impacts of objective function on rpl-routing protocol: a survey. In: 2021 Sixth international conference on wireless communications, signal processing and networking (WiSPNET), pp 251–255. IEEE

Don J, Alfred M, Scott V (2001) The elliptic curve digital signature algorithm (ECDSA). Int J Inf Secur 1(1):36–63

Ensworth JF, Reynolds MS (2017) Ble-backscatter: ultralow-power iot nodes compatible with bluetooth 4.0 low energy (ble) smartphones and tablets. IEEE Trans Microwave Theory Techniques 65(9):3360–3368

Ghada G, Aref M (2019) 6lowpsec: an end-to-end security protocol for 6lowpan. Ad Hoc Networks 82:100–112

Gupta M, Singh S (2020) A survey on the zigbee protocol, it's security in internet of things (iot) and comparison of zigbee with bluetooth and wi-fi. In: Applications of artificial intelligence in engineering: proceedings of first global conference on artificial intelligence and applications (GCAIA 2020), p 473. Springer

Hannes T, Emmanuel B (2019) Cyberphysical security for the masses: a survey of the internet protocol suite for internet of things security. IEEE Secur Privacy 17(5):47–57

Jacobovitz O (2016) Blockchain for identity management. The Lynne and William Frankel Center for Computer Science Department of Computer Science. Ben-Gurion University, Beer Sheva

Jetmir H, Eli DP, Ingrid M, Jeroen H (2018) A survey of lorawan for iot: from technology to application. Sensors 18(11):3995

Kalyani G, Chaudhari S (2020) Survey on 6lowpan security protocols in iot communication. In: ICDSMLA 2019, pp 696–702. Springer

Kanakaris V, Papakostas GA (2020) Internet of things protocols-a survey. Int J Human Technol 1(2):101–117

Karalis A, Zorbas D, Douligeris C (2018) Collision-free broadcast methods for IEEE 802.15, 4-tsch networks formation, pp 91–98

Khusanbek G, Tai-Myoung C (2019) Comprehensive survey on internet of things, architecture, security aspects, applications, related technologies, economic perspective, and future directions. J Inf Proces Syst 15(4):797–819

Kim H-S, Ko J, Culler DE, Paek J (2017) Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): a survey. IEEE Commun Surv Tutor 19(4):2502–2525

Kinza Shafique, Bilal A Khawaja, Farah Sabir, Sameer Qazi, and Muhammad Mustaqim. Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios. *IEEE Access*, 8:23022–23040, 2020

Krejčí R, Hujňák O, Švepeš M (2017) Security survey of the iot wireless protocols. In: 2017 25th Telecommunication Forum (TELFOR), pp 1–4. IEEE

Lihua L, Shangping W, Bintao H, Duo Z (2019) A keyword-searchable ABE scheme from lattice in cloud storage environment. IEEE 7 Access 109038–109053

Limei He, Zheng Yan, Mohammed Atiquzzaman (2018) Lte/lte-a network security data collection and analysis for security measurement: A survey. IEEE Access 6:4220–4242

Marco L, Francesco P, Domenico S (2021) Internet of things: a general overview between architectures, protocols and applications. Information 12(2):87

Marksteiner S, Juan Expósito Jiménez V, Valiant H, Zeiner H (2017) An overview of wireless iot protocol security in the smart home domain. In: 2017 Internet of Things business models, users, and networks, pp 1–8. IEEE

Mavromatis A, Colman-Meixner C, Silva AP, Vasilakos X, Nejabati R, Simeonidou D (2019) A software-defined iot device management framework for edge and cloud computing. IEEE Internet of Things J 7(3):1718–1735

Naidu GA, Kumar J (2019) Wireless protocols: Wi-fi son, bluetooth, zigbee, z-wave, and wi-fi. In: Innovations in electronics and communication engineering, pp 229–239. Springer

Nastase L (2017) Security in the internet of things: a survey on application layer protocols. In: 2017 21st international conference on control systems and computer science (CSCS), pp 659–666. IEEE

Rajashree S, Soman KS, Gajkumar Shah P (2018) Security with ip address assignment and spoofing for smart iot devices. In: 2018 international conference on advances in computing, communications and informatics (ICACCI), pp 1914–1918. IEEE

Raposo D, Rodrigues A, Sinche S, Silva JS, Boavida F (2018) Securing wirelesshart: monitoring, exploring and detecting new vulnerabilities. In: 2018 IEEE 17th International symposium on network computing and applications (NCA), pp 1–9. IEEE

Salman T, Jain R (2019) A survey of protocols and standards for internet of things. arXiv preprint. arXiv:1903.11549

Savvidina Auliva R, Sheu RK, Liang D, Wang W-J (2018) Iiot testbed: a dds-based emulation tool for industrial iot applications. In: 2018 International conference on system science and engineering (ICSSE), pp 1–4. IEEE

Sharma P, Kherajani M, Jain D, Patel D (2020) A study of routing protocols, security issues and attacks in network layer of internet of things framework. In: 2nd International conference on data, engineering and applications (IDEA), pp 1–6. IEEE

Soni D, Makwana A (2017) A survey on mqtt: a protocol of internet of things (IoT). In: International conference on telecommunication, power analysis and computing techniques (ICTPACT-2017), vol 20

Sowmya KV, Teju V, Pavan Kumar T (2021) An extensive survey on iot protocols and applications. In: International Conference on Intelligent and Smart Computing in Data Analytics, vol 1312, 131

Terán M, Aranda J, Carrillo H, Mendez D, Parra C (2017) Iot-based system for indoor location using bluetooth low energy. In: 2017 IEEE Colombian conference on communications and computing (COLCOM), pp 1–6. IEEE

Urien P (2017) Introducing tls/dtls secure access modules for iot frameworks: concepts and experiments. In: 2017 IEEE symposium on computers and communications (ISCC), pp 220–227. IEEE

Winter T, Thubert P, Brandt A, Hui JW, Kelsey R, Levis P, Pister K, Struik R, Vasseur J-P, Alexander RK et al (2012) Rpl: Ipv6 routing protocol for low-power and lossy networks. RFC 6550:1–157

Xuanxia Y, Zhi C, Ye T (2015) A lightweight attribute-based encryption scheme for the internet of things. Fut Gener Comput Syst 49:104–112

Yang Y, Xianghan Z, Chunming T (2017) Lightweight distributed secure data management system for health internet of things. J Netw Comput Appl 89:26–37

Zhang P (2018) A survey on the security of coap and xmpp and their performance comparison

Zhang Y, Weng J, Dey R, Jin Y, Lin Z, Fu X (2020) Breaking secure pairing of bluetooth low energy using downgrade attacks. In: 29th {USENIX} Security Symposium ({USENIX} Security 20), pp 37–54

Chapter 5
Communication Security in IoT

Raveena Yadav and Vinod Kumar

Introduction

There was a time when no standard and technology was present for doing communication among the computers. Then, in 1983, Internet has come; it is also known as the birthday of the Internet. It was invented by Tim Berners Lee. The Internet provides a lot of features in which most beneficial is communication. This helps in sending information from one device to another. With the help of communication, the device-to-device and device-to-human beings can communicate and build a network that is known as Internet of Things (IoT). This communication carries the data which may include sensitive information, and this makes it vulnerable to attackers. Maintaining the communication secure and reliable, there is a need of identifying the protocols against the requirement of the application and attacks on IoT devices and most important producing a defense mechanism against them.

For maintaining and building this complex network, there is a requirement of architecture. It makes it easy to build applications of IoT. But, to date, IoT does not have any standard architecture. In this chapter, we have referred to three-layered architecture (Sidna et al. 2020): perception layer, communication layer, and the topmost layer is service layer. Perception layer helps in sensing and gathering the data. The main components of this layer are sensors, actuators, and radio frequency identification devices (RFIDs). Sensors gather the data; actuator task is doing action, and RFID helps in providing unique identification to devices. The elements used in this layer are low powered and resource constrained. It makes them difficult to manage and makes them energy efficient. Communication layer, the main task of this layer is transferring data from the perception layer to the application layer. It also helps in connecting the different nodes of the network of IoT. For transferring information, this layer uses different network protocols. ZigBee protocol has a short physical range and its name, came from the way of flying the bees. 6LoWPAN combines

R. Yadav (✉) · V. Kumar
Delhi Technological University, Delhi, India
e-mail: raveenakyb@gmail.com

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_5

with IPv6 for providing addressing to different nodes as IPv6 is a heavy protocol that consumes more resources in comparison to 6LoWPAN. The elements used in IoT networks are low powered, so they also require protocols that consume less energy and do work in a resource-constrained environment. BLE is the next version of Bluetooth, but it works on low-energy components with a good data rate. NFC is one protocol where the application requires working in a small area. This protocol uses magnetic induction for transferring information from one node to another, and this works in the small range. Sigfox protocol is a long-range protocol, it covers a large geographical area of approximately 50 km. Except for these protocols, there is a large number of protocols present for communication among different node. The selection of these protocols depends on the application of IoT devices. If the device requires working in a large area, then it will go for long-range protocols, and if it requires working in short range then it will go for short-range protocols like NFC.

For providing different services by IoT devices, communication among devices and elements used in IoT is very important. This purpose is fulfilled by different communication protocols as mentioned above some of the protocols. In this chapter, we will discuss these protocols.

IoT helps in giving a comfortable life, and for providing this feature, sometimes, it requires our confidential data or some data from which attackers can take advantage. Because of this problem, security is one of the major issues for maintaining a reliable IoT network. There are a few terms and things that are very important to maintain security like confidential, integrity, authentication, availability, and non-repudiation. In confidentiality, our confidential data such as bank details should be safe from the attacker by different cryptography or end-to-end encryption mechanism. When data are moving from one place to another, it should not be altered by anyone. The same data that are given by the source node should be sent same to its destination address. This comes under the maintaining of the integrity of data. If the device accepts data without knowing that the device is sending from its network or it is an outsider node, then it will create a security issue in the IoT network. This is the problem of authentication, and it can be maintained by using a pair of keys which can be maintained by a control certification authority. A malicious node sends data to a legitimate node. If a malicious node denies that it has sent this data, then it will create a problem with non-repudiation. For maintaining this, there is a requirement of a hash function with the digital signature of the source node. There are different types of attack that can be done by the attacker; in the second section of this chapter, we have given a light to types of attack in communication and have also provided some defense mechanisms.

As day by day, connections among IoT devices are increasing. Each device produces some amount of data and managing, analyzing, and storing data are challenges related to data produced by devices. This massive amount of data can reduce the performance of the network. It also increases the load on the network or increases the traffic in the network and also uses more resources to maintain the reliability of the network. For efficient use of the network, there is a requirement for network optimization. In the last section of this chapter, we have mentioned a comprehensive view of network optimization in IoT. Researchers have given different approaches and algorithms for network optimization. In network optimization, there are several challenges are also present such as heterogeneity of network requires more energy as a comparison to homogenous network. Maintaining a dynamic routing table also increases the load of the network; connection with the new device also requires more resource, energy, increase the load, and require security. These challenges are also mentioned in the last section of this chapter.

Chapter Organization

This chapter is divided into six sections; the first section is about different communication protocols. In this, we have discussed the importance of communication protocols, different protocols such as ZigBee, Bluetooth low energy, near-field communication, 6LoWPAN, Wi-Fi, Sigfox, and the comparison of these protocols. In the second section, we have discussed about the attacks in communication layer such as sinkhole, wormhole, black hole, flood rank. In the third section, we have mentioned some of the defense mechanisms like content chaining scheme, authentication defense mechanism, intrusion detection system, and end-to-end encryption and the importance of defense in IoT networks. The fourth section is about the importance of network optimization and different techniques for optimization of the network. In the fifth section, challenges faced in network optimization such as mobility, routing, heterogeneity, and many others. The last section is about the conclusion of the chapter (Fig. 5.1).

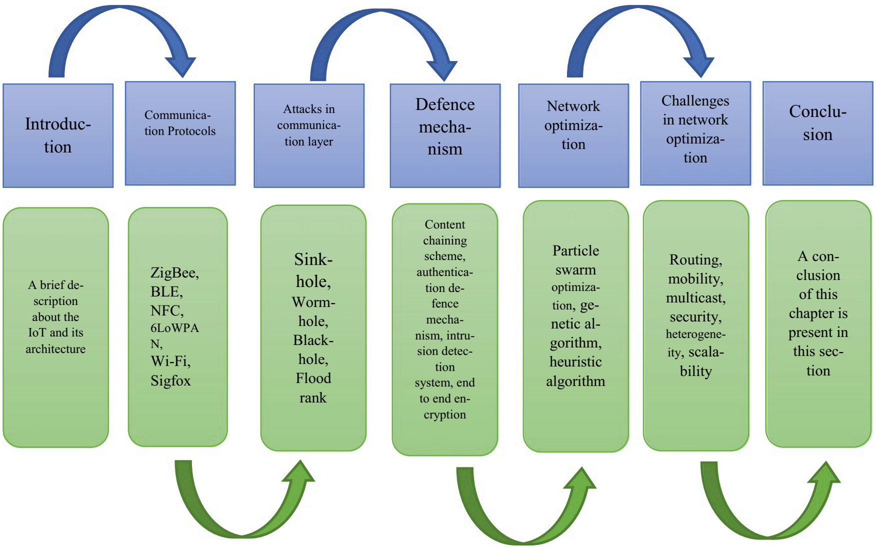

Introduction
Communication Protocols
Attacks in communication layer
Defence mechanism
Network optimization
Challenges in network optimization
Conclusion
A brief description about the IoT and its architecture
ZigBee, BLE, NFC, 6LoWPAN, Wi-Fi, Sigfox
Sinkhole, Wormhole, Blackhole, Flood rank
Content chaining scheme, authentication defence mechanism, intrusion detection system, end to end encryption
Particle swarm optimization, genetic algorithm, heuristic algorithm
Routing, mobility, multicast, security, heterogeneity, scalability
A conclusion of this chapter is present in this section

Fig. 5.1 Organization of chapter

5.1 Different Communication Layer Protocols and Mediums for IoT

IoT can be viewed as the next version of the Internet, which is still in its developing stage. IoT makes a network of IoT devices and integration of a different network of IoT. These devices exchange information among them and make intelligent decisions. For doing communication among devices, it requires a medium; this can be wireless or wired. But, nowadays, we are moving forward and adopting wireless networks. From this, device can be managed and visualize its work when we are not present with the device. This communication is a little different; as, in this network, device-to-device communication is also present along with human-to-device communication. This network depends on two terms anywhere and anytime. From this, we can say that IoT is based on ubiquitous computing.

For exchanging the information, it requires different protocols. Researchers have already provided many protocols for transmitting the message from one node to another. There are still many more protocols are yet to come. TCP/IP protocol suite is already available for communication via the Internet. That has five layers: physical layer, data link layer, network layer, transport layer, and application layer. But, this protocol stack is not able to work with the devices and components of IoT. As TCP/IP protocol suite does not help in managing the heavy load of low power devices. Most of the devices of IoT are mobile and have a connection of heterogeneous devices. In these, using TCP/IP is a little difficult as these devices are low in power, low in memory, and resource constraint in nature. In generally, TCP/IP protocol suite used in high power devices.

In this section, we will see the protocols that have been used in transferring information from one smart device to another. These protocols are chosen according to the need for the application of the IoT. The requirement of IoT devices or applications can be categorized in terms of security, data rate, and range. There are different issues present in IoT networks. In these issues, security is major in the communication layer as the communication layer carries a lot of data with including confidential data. Saving this data from intruders and eavesdroppers is a challenging task. Attackers try to break these protocols and try to harm the device of IoT. They do different attacks on the device. It is very difficult to mention all attacks in a single chapter. So, in this section, we have taken major attacks done by the attacker. Defenders have also provided different defense mechanisms of attack. In this chapter, we have also discussed the different defense mechanism (Fig. 5.2).

5.1.1 ZigBee

With the growth of IoT devices, there is a requirement for a communication protocol that can handle the communication among many numbers IoT devices. ZigBee protocol is one of them. This protocol is developed by the ZigBee alliance. Its name

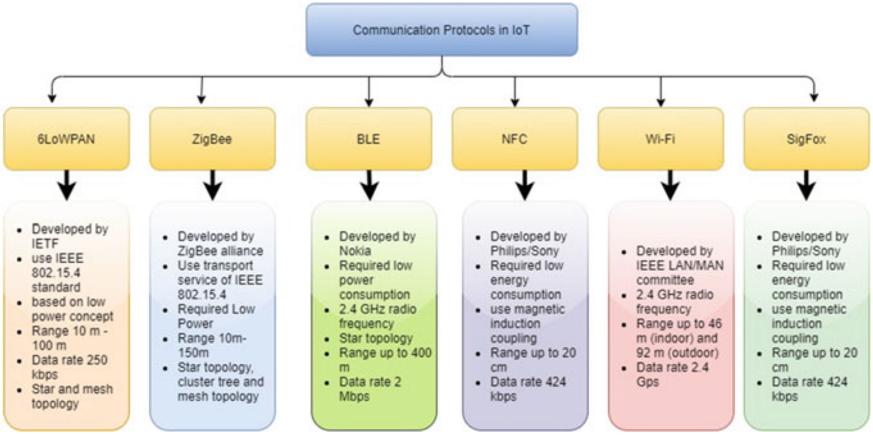
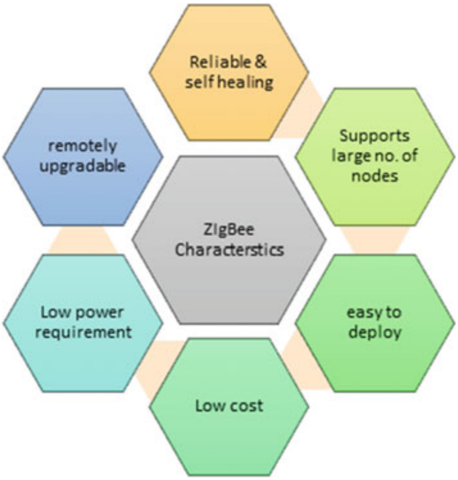

Communication Protocols in IoT
6LoWPAN
ZigBee
BLE
NFC
Wi-Fi
SigFox
• Developed by IETF
• use IEEE 802.15.4 standard
• based on low power concept
• Range 10 m - 100 m
• Data rate 250 kbps
• Star and mesh topology
• Developed by ZigBee alliance
• Use transport service of IEEE 802.15.4
• Required Low Power
• Range 10m-150m
• Star topology, cluster tree and mesh topology
• Developed by Nokia
• Required low power consumption
• 2.4 GHz radio frequency
• Star topology
• Range up to 400 m
• Data rate 2 Mbps
• Developed by Philips/Sony
• Required low energy consumption
• use magnetic induction coupling
• Range up to 20 cm
• Data rate 424 kbps
• Developed by IEEE LAN/MAN committee
• 2.4 GHz radio frequency
• Range up to 46 m (indoor) and 92 m (outdoor)
• Data rate 2.4 Gps
• Developed by Philips/Sony
• Required low energy consumption
• use magnetic induction coupling
• Range up to 20 cm
• Data rate 424 kbps

Fig. 5.2 Communication protocols in IoT

came from bees and the way it moves like zig and zag; these bees help the other bees in giving information where nectar is present. This same concept has been used in this protocol. It uses IEEE 802.15.4 standard for transmitting the message. This standard supports a time slot for transferring the message and helps to support secure communication. For transferring the message, it also supports different topologies such as star topology, peer-to-peer network, and cluster tree network. These topologies are used by the ZigBee protocol. This protocol came into the use of an IoT network because of its low power consumption in comparison to Wi-Fi. It also helps in connecting a large number of nodes in a single network, and this network can be extended by routers. Thus, it is beneficial for IoT networks to connect a large number of devices and expand the network (Fig. 5.3).

Fig. 5.3 ZigBee characteristics



ZigBee devices can be categorized into two types based on the processing of data. The first type is a physical device; it can also be further divided into two types; they are fully functional device (FFD) and reduced function device (RFD). The fully functional device has the capability of working as a network coordinator, and sometimes, it acts as RFD. RFD can never be a network coordinator, while it can communicate to the network coordinator. Most of the time, it acts as an end node, which helps in making a network cost-effective. There is one disadvantage of using RFD as is it works only in star topologies, whereas FFD can work in any topologies of ZigBee (star, mesh, and cluster tree) as shown in Fig. 5.4. The second type is a logical device; if we further categorize them, they are coordinator, which helps an identification to the nodes. Router, they help in transmitting the data with that it also helps in increasing the network area. Another one is end devices that help in getting the information from the sensor as the sensor helps to collect the data from its surrounding. These end devices help to proceed with the process. This protocol has two access modes; one is the beacon, in which a time slot presents and helps in increasing the lifetime of the battery. The other one is a non-beacon which does not have a time slot. This access mode is helpful for the network coordinator.

It is a lightweighted protocol and mostly uses a tree approach for routing the data. Because of this characteristic, IoT devices can communicate with less energy consumption. This protocol has one limitation, while following tree-based topology is that it suffers from an orphan node issue. This problem occurs because for transferring messages, it uses distributed address assignment mechanism (DAAM). In this mechanism, it set some variable such as *depth_of_tree*, *limit_of_children*, *limit_of_router,* and only *one_coordinator* use in a network area. Z-coordinator helps in maintaining the network and acts as ahead of the network, all other components router, and end devices send information to its coordinator for further processing. Some researchers (Sidna et al. 2020) have given an approach for solving this issue by shifting the orphan node, and this node can send a message to its neighbor, and its child that in the future, it can be turned into an orphan node. Dizdarević et al. (2019) use

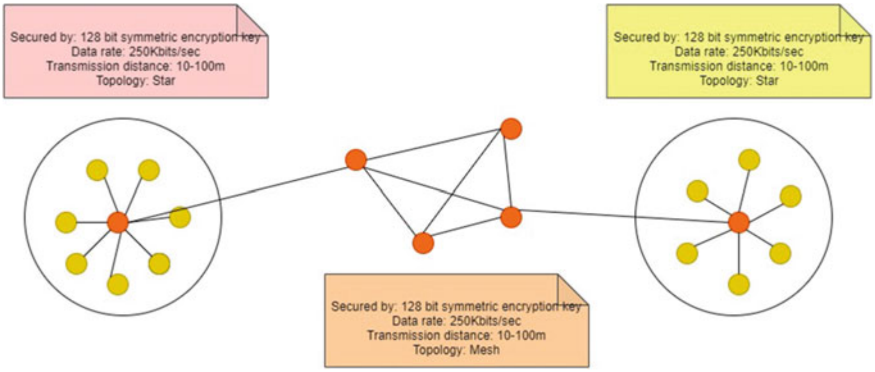

Secured by: 128 bit symmetric encryption key
Data rate: 250Kbits/sec
Transmission distance: 10-100m
Topology: Star
Secured by: 128 bit symmetric encryption key
Data rate: 250Kbits/sec
Transmission distance: 10-100m
Topology: Star
Secured by: 128 bit symmetric encryption key
Data rate: 250Kbits/sec
Transmission distance: 10-100m
Topology: Mesh

Fig. 5.4 View of ZigBee working

computational approach with probability. This approach is 6% more efficient than standard ZigBee (Failed 2020). This protocol gives a better result in the short area even it is a long-range protocol as deploying nodes in this network is a complex task. Ramya et al. (2011) have used a combination of ZigBee and Wi-Fi protocol in the home automation system, in which a gateway has been used for connecting these two protocols. ZigBee coordinator takes data from the Wi-Fi sensor node and performs its function.

With all these characteristics of ZigBee, IoT devices can function for a long time. In consideration of power-consumption issue, Li et al. (2018) introduced passive ZigBee. This variant of protocol consumes less power in comparison to conventional ZigBee. There is another method of improvement of this protocol.

Researchers have used the ZigBee protocol in various applications of IoT. Researchers have introduced the ZigBee protocol in the medical health sector (Li et al. 2018). In this, nodes are connected with the help of this protocol and collect data. After the collection of data, they used analysis techniques also. This protocol helps in collecting the data of remote patients. It used ZigBee and RFID; RFID helps in giving the identification to nodes, and ZigBee helps in finding the node in the long-range area. It also gives a comparison of using ZigBee and Wi-Fi protocol. Authors have discussed the security mechanism in ZigBee protocol (Safaric and KresimirMalaric 2006). This mechanism is divided into two parts. The first is finding the authentic nodes of the network. The second is stopping the theft and alteration of data done by the attacker. Authors have mentioned the attack on Philips smart bulb, in which a worm is needed to introduce on a single bulb (Aju 2015). Then, this worm will hop from one bulb to another via ZigBee protocol. In this attack, the attacker can handle the whole city light with this worm. Rashid et al. (2016) smart_scene application has mentioned in which use of RFID and ZigBee protocol is used. Nodes are dynamic.

Characteristics of ZigBee Protocol

(1) It uses three frequency bands for different areas and different applications: 2.4 GHz, 868 MHz, 915 MHz.
(2) It has long-day battery life (3 months–20 years).
(3) It can connect a large number of nodes in a single network.
(4) It follows star topology, cluster technique, mesh topology.
(5) It is based on low memory and storage capacity.
(6) It has a low data rate in comparison to other protocols (250 kbps).

Challenges in ZigBee Protocol

(1) The network that is using ZigBee protocol making it *energy_efficient* is a challenge as nodes are battery-powered nodes. If the battery died, then it will break the link for transmission. This can be improved by using solar cells in the node. This can be possible only when the device is present in the lighted area.
(2) This protocol covers a large area of the network. There is the possibility that nodes are present in a harsh environment. So, self_management of this network is one of the challenges.

(3) The connection of nodes in ZigBee protocol is already in a large number even if any node wants to enter into the network. This can also create a challenge for *connecting_new_node* at a place where it consumes less energy.

(4) All communication protocols generate a huge amount of data, maintaining and providing *security* for this data is a very critical task. These protocols are prone to various attacks.

5.1.2 BLE

In starting phase of the IoT network, Bluetooth was used as a communication protocol. It helps in transmitting the data from one node to another. For this, it uses radio waves, and its range is approximately 400 m, depending on obstacles. As the number of IoT devices is increasing day by day with decreasing the battery power. So, Bluetooth low energy was introduced by the company Nokia. It consumes less power in comparison to conventional Bluetooth and is more suitable for IoT devices in respect of increasing the lifetime of the device. It also uses radio waves for transmitting data with a frequency of 2.4 GHz. It has also reduced the channels used in Bluetooth from 79 to 40.

BLE uses the master and slave method in which one node acts as a master and other nodes act as slaves. A master can have any number of slaves, whereas a slave can have only one master. So, the topology used in this protocol is star topology as shown in Fig. 5.5. For making it more energy efficient, it uses TDMA in which nodes will be given a time slot in which the node can transmit its message to its master. Slave nodes remain awake only its time slot. This helps in saving energy and increasing the battery life.

BLE uses two packets format; one is a data packet, and the second is an advertising packet as shown in Fig. 5.6. These packets have 1 byte for preamble which helps in the synchronization of data in the aspect of time and frequency. Next is the access address of 4 bytes, which helps in accessing the data. The advertising packet broadcasts the packet, so it uses a fixed access address, 0 × 8E89BED6. The device which uses BLE for transferring the data generates a random number in its initial phase. This value is used in making a connection request, and it is stored in the access-address

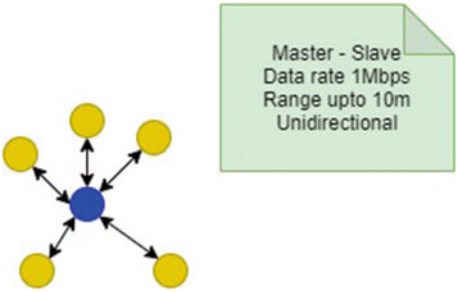


Fig. 5.5 BLE features

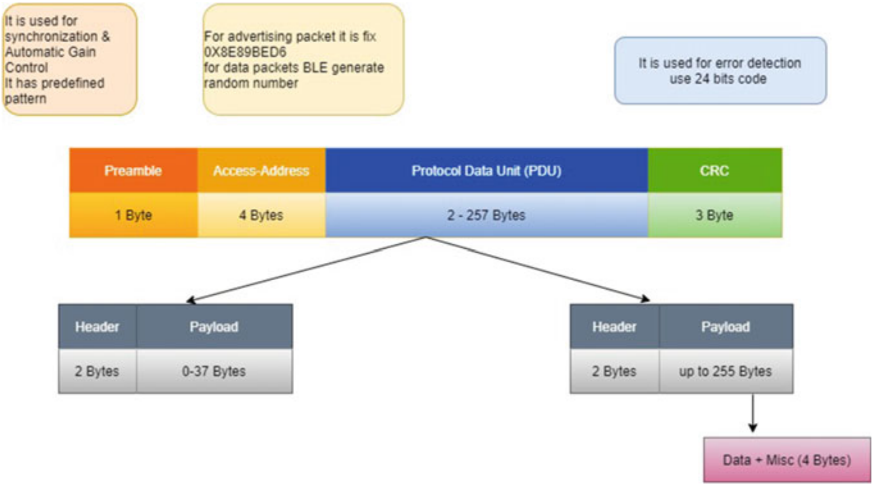

It is used for synchronization & Automatic Gain Control
It has predefined pattern
For advertising packet it is fix 0X8E89BED6
for data packets BLE generate random number
It is used for error detection use 24 bits code
Preamble
1 Byte
Access-Address
4 Bytes
Protocol Data Unit (PDU)
2 - 257 Bytes
CRC
3 Byte
Header
2 Bytes
Payload
0-37 Bytes
Header
2 Bytes
Payload
up to 255 Bytes
Data + Misc (4 Bytes)

Fig. 5.6 BLE packet format

field. The next field is the protocol data unit; it helps in identifying whether the packet is an advertising packet or data packet. The last field is cyclic redundancy code (CRC) which is used for finding the error (if data have changed before reaching to destination location). It uses a 24-bit code for error detection.

BLE protocol uses basic components of standard Bluetooth (Nieminen et al. 2014). The changes are built for making it a low power-consumption protocol. The number of channels has been reduced from classic Bluetooth to BLE. Researchers have proposed a food monitoring system via BLE. In their model, they have used three sensors: gas sensors, humidity sensors, and temperature sensors. Gas sensors help in checking the gas in which food items are stored and gas produced by any food item. The humidity sensor senses the humidity level surrounding the food items. Temperature sensors check that food item has been stored incorrect temperature or there is need of change. All data produced by these sensors have been transferred to the application of a food monitoring system via BLE. Authors have mentioned about Blue_voice application, in which devices of IoT communicate via BLE (Venkatesh et al. 2017). A lot of devices need to connect, for this; there is a need for the discovery of neighbors. Discovering of neighboring is divided into two types: active discovering and passive discovering; these are known as scanner and advertiser, respectively. They use two bottom layers for transmitting and receiving the data and error control and flow control.

Researchers have shown the implementation of BLE in various applications of IoT. E-health system uses BLE for communication and transmitting data (Hortelano et al. 2017). For saving utilization of power in home, BLE has used. This protocol is beneficial for IoT as it is an integration of low-power communication and mobile computing. For better performance of the vehicle, they are connected via BLE (Gentili et al. 2016). The ticket system has been built using BLE. Traffic light system management can be maintained by BLE (Mackensen et al. 2012). Smart wearables are connected and send information to the application via BLE. The smart museum can be built with the help of an IoT network and the utilization of the BLE protocol for sending information about the items presented in the museum. With the advancement in every sector, aquaculture is also improving. Smart aquaculture is maintained by BLE.

Characteristics of BLE

(1) For setting up the connection, it requires less amount of energy. Overall, it consumes low energy.
(2) It has a good data rate for the transmission of data.
(3) It connects a smaller number of nodes in a network.
(4) It has more storage than the ZigBee protocol, 100 KB.
(5) It covers a smaller area for transmission.
(6) It uses the AES encryption method for security.

Challenges and issues in BLE

(1) Setting the connection, first, requires a setup phase.
(2) It works only in the short-range area.
(3) Most of the devices are based on standard Bluetooth.
(4) This protocol helps only transmit smaller size packets.

5.1.3 Near-Field Communication

For sending data from one node to another, numerous protocols are present. But, there is only one protocol that is based on short-distance communication. This protocol is known as near-field communication (NFC). It is a comparative protocol to Bluetooth low-energy protocol. As both these protocols are based on short-range communication, but, NFC has a shorter range than BLE. The distance between nodes is up to 210 cm in NFC. As its name suggests that it does communicate when the device is near to another communicating device. The devices used magnetic induction coupling for communication; in this, devices should be close to each other. Because of this short range, there is very little chance that data would be modified by some intruder. In terms of security, it is much better than BLE.

The frequency band used by this protocol is 13.56 MHz; it has modes for transmitting the data from one device to another. The data rate is in the range of 212–424 kbps. One is active mode, in which both devices generate their radio waves for transmitting the message. The devices which follow active mode get power supply from some source. Another mode is the passive mode, in which devices have their battery. In this, only, one device initiates its radio waves for transferring messages other one uses load modulation. In comparison to the data rate with BLE, it has less speed, but it does not require any pairing system like in BLE. NFC setup time is very less in comparison to BLE.

Example of NFC in IoT; a smart lock in the room can be managed by NFC protocol. A card with NFC can be used as a key for locking the room. A smartphone with NFC can be used to unlock the room. If a person comes close to the lock that is locked by an NFC card, then only the lock will open.

Authors have proposed a model for teacher staff rooms using NFC protocol (Gonzalez et al. 2008). In this, person use a mobile device with the contact of staff room's door and identify teacher is available in room or not. In this, researchers have divided their approach into different stages (Dominikus and Aigner 2007). This protocol is very useful where short-range communication requires like a car or any other vehicle can be unlocked by using NFC protocol. When the device comes in a range of the vehicle, then the NFC device asks wants to unlock the car. So, this protocol is useful where locking and unlocking systems require. The trending ATM cards are coming with this protocol. In which, there is no requirement of swiping the card, only required to come in its range. Smart wearable senses our body and collects and disburses the data to the application. Gonzales (2012) has introduced m-coupon as shown in Fig. 5.7. In this, the coupon is present on paper; from the NFC device, the coupon can be used. In smart shopping, NFC devices can be used. As user needs to download the app, from which, he wants to shop. Then, he will add items into the cart and make payment. He goes to the shop and puts his NFC device near to shop's NFC device. Then, on his mobile phone, he gets guidance on where he finds his product.

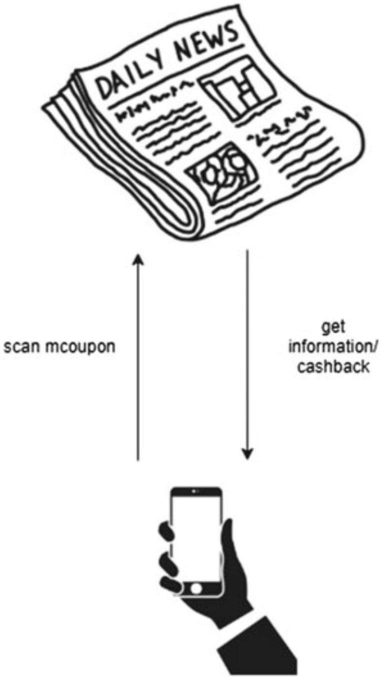


Fig. 5.7 NFC using in m-coupon

Characteristics of Near-Field Communication Protocols

(1) It consumes low energy in comparison to other communication protocols.
(2) It uses magnetic induction for transmitting data.
(3) It does not require a setup phase as a Bluetooth protocol.
(4) It uses high speed for sending data, 20–200 Mbps.

Challenges and Issues in Near-Field Communication Protocols

(1) It covers a short-range area.
(2) It has some security issues such as a man-in-middle attack, data corruption, and eavesdropping.
(3) It is the lack of standardization to the application level.

5.1.4 6LoWPAN

There are different communication protocols are present in IoT networks for making reliable and sustainable communication between massive numbers of nodes. Because of this huge number, IPv6 was used over IEEE 802. 15.4; it helps in giving a unique address to nodes. This was named 6LoWPAN (Low-power wireless personal network). The motivation for designing this protocol is that the TCP/IP protocol suite is not suited for low-power and resource-constrained devices. TCP/IP requires a lot of energy, memory, and resource in comparison to 6LoWPAN. It was designed by the Internet Engineering Task Force (IETF).

This protocol has three main components that are host node, which helps to take the information from the environment and transfer it to the next component. The topology used in the host node network is mesh topology. In this, host nodes can communicate among themselves. The next component is the router node; these nodes make a network as a bridge between two nodes (host node and edge node). It helps in transferring the message from the host node to the end node. The third crucial component is the end node; it helps in managing the load of data.

Routing protocols used in this protocol are categorized into two types: mesh under and route over. Mesh under makes a packet of data and sends it through a different route. The frame size used by this protocol is 127 bytes. This protocol also uses the fragmentation method to send data over IEEE 802.15.4 standard. It also uses the header compression technique, and for identifying the destination node, it used a 16-bit address. When data reach its destination, it reassembles all the packets. In route over, routing technique is decided by network layer of 6LoWPAN architecture. This protocol uses the packet filtering method; this helps in accepting and discarding a packet from unauthentic sources or to authentic receivers. Various stacks of 6LoWPAN are mentioned in Al-Kashoash et al. (2019) as shown in Fig. 5.8.

One of the major issues of IoT is security; this protocol helps in providing security by using AES 128 bit. In this, it uses an encryption method and authentication scheme. Because of these two features, there is very little chance of eavesdropping and altering the data in the wireless sensor networks.

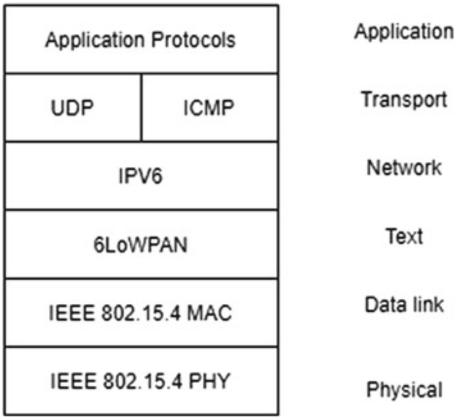


Fig. 5.8 Layered structure of 6LoWPAN

The main challenge of using this protocol is it does not have any collision detection and avoidance scheme. If any collision occurs, it will not be able to predict and avoid the collision; this makes more energy consumption in the network. The other disadvantage, it does not support mobility. Mobility is supported by Sigfox; about this, we will read in the next section. The other disadvantage is it covers less area. For covering a large geographical area, then, a massive number of 6LoWPAN devices are required. It requires a complex routing protocol that consumes more energy and using such many devices increases its cost.

Characteristics of 6LoWPAN Protocol

(1) It has a packet filter feature.
(2) It works with IPv6 and IEEE 802.15.4.
(3) It works in mesh and star topology.
(4) This protocol works with three components are as follows: source router, intermediate router, and end-node router.
(5) It consumes less energy.

Challenges and Issues in 6LoWPAN Protocol

(1) Maintaining security in the network using the 6LoWPAN protocol.
(2) Preventing devices from denial-of-service attack.

5.1.5 Wi-Fi

In the evolution of wireless networks, Wi-Fi plays a very important role in transmitting messages. Most of the devices are connected to Wi-Fi. This protocol is one of the oldest protocols. It has started at the time when the Internet has introduced some connectivity and transmitted information from one system to another. There are many protocols are available for sending information; Wi-Fi is one of them. Wi-Fi has more data rate in comparison to other protocols. This protocol also works in TCP/IP protocol stack. The data rate of this protocol is 300 Mbps. It can send data in less time. This helps in increasing its throughput rate. ZigBee is a long-range protocol, but Wi-Fi provides more range than it. It helps in covering more areas than ZigBee. It can cover approx. 400 in outside and 200 in inside. It gives less effect on data rate in comparison to other protocols. One more advantage of this protocol is, this, there is no need for line-of-sight transmission require. The wireless network has provided wireless sensors that can be connected via Wi-Fi. In this, sensors do not require a central authority for transferring the message. With this, this protocol also helps the IoT in providing green communication. Sharma et al. have introduced light fidelity (Li-Fi) for communication in IoT network.

Nowadays, we can see our smart phones are connected to Wi-Fi most of the time. In houses, we have smart lights; a smart refrigerator and many other items are available, and all are connected via a Wi-Fi network. This protocol can cover a significant area for transmitting data. For increasing the area range, routers can be used. Researchers have given various IoT applications that are connected via Wi-Fi. Authors have described the availability of Wi-Fi sensors (Li et al. 2011). Home automation system, in which, all devices such as geyser, coffee maker, refrigerator, smart air conditions all are connected with the help of Wi-Fi network. The smart medical sector, in which, track of patient is done by Wi-Fi (Cheng and Chang 2017).

Characteristics of Wi-Fi protocol in the Internet of Things

(1) It has a high data rate for sending information, 300 Mbps.
(2) It has great throughput as it has a high data rate. So, it can send data in a very less amount of time. This helps in increasing the throughput value.
(3) It covers a large area. This protocol is reliable for sending data when the distance between two nodes is large.
(4) It does not require the presence of nodes in a line-of-sight manner.

Challenges and issues in Wi-Fi protocol

(1) Maintain security and privacy among nodes.
(2) Management of huge data produced by nodes.
(3) Management of nodes that is present at a far distance.

5.1.6 Sigfox

As day by day, our dependency on electronic and smart devices is increasing day by day. These devices are also getting improved as they use low energy consumption that helps to increase the battery life of the device. Different communication protocols are helping to achieve this aim. Sigfox is one of the trending communications protocols. It was designed by one of the French companies known as IoT valley. This protocol was given by two persons: Ludovic Le Moan and Christophe Fourtet. It has already covered a large geographical area of 5.8 million square kilometers. Concerning this, it has also been used in more than 70 countries. The main aim of this protocol is to connect a huge number of devices in the wireless network. For transmitting data among different devices, it consumes less amount of energy even obstacles are present in the network area. It uses a single-hop routing method (star topology) which also helps in saving energy.

This protocol is the future of the Internet of Things because it covers large geographical areas with less consumption of power and bandwidth. This protocol used an ultra-narrow band scheme, in which it can send data up to 50 km by using a low-powered battery. One more advantage of using UNB is it helps in gathering the original signal by avoiding the noise signal from surrounding and using less bandwidth for transferring data. In conventional Sigfox, only, uplink communication was supported, but now in the updated version of protocol support both uplink and downlink communication.

While deploying this protocol, network dimension has great importance as it covers a large area, and the base station helps to increase the area. So, proper dimension helps to increase more efficiently.

The issue in this protocol is it is the less favorable protocol where security and downlink communication have more priority than other features. It uses three frequency bands for transmission. It also helps in the reliability of the network as the sink node will be able to receive packets even if a collision occurs between two nodes. It provides better performance outside (Ribeiro et al. 2018).

Characteristics of Sigfox protocol

(1) The bandwidth is used for this protocol is 100 and 600 bps.
(2) It has its standard.
(3) It uses frequency band 868 MHz at EU and 902 MHz in the USA.
(4) It mostly follows a star topology.

Challenges and issues in Sigfox protocol

(1) Spoofing attack on Sigfox protocol.
(2) No authentication mechanism in this protocol.
(3) Confidential information stored on node.

From Table 5.1, we can find the appropriate protocol for communication among IoT devices.

5.2 Communication-Level Attacks

In this technical world, the connection of smart devices is increasing, and features provided by these devices are also increasing; concerning these, issues in IoT networks are increasing. There are many issues present in IoT networks such as security, big data, maintaining networks among heterogeneous devices, and energy consumption. Among this, security is a major concern. IoT devices take information from the environment, and sometimes, they also take data from the user. The data can be confidential. Elements present in IoT networks transfer data from one device to another wirelessly, and confidential data are also transferred via the wireless network.

Table 5.1 Comparison between communication protocols

Characteristics	Sigfox	6LoWPAN	ZigBee	NFC	BLE
Year	2009	2015	1998	2011	2010
Standard	Own, proprietary	IEEE 802.15.4	IEEE 802.15.4	JIS X-6319–4	IEE 802.15.1
Frequency band	868 MHz (EU) 902 MHz (USA)	2.4 GHz	2.4 GHz	125 kHz 13.56 MHz	2.4 GHz
Data rate (kbps)	100 bps/600 bps	250 kbps	250 kbps	212 Kbps 424 kbps	1 Mbps
Network topology	Star	Star, mesh	Star, mesh, cluster	P2P network	Star-bus network
Power	100mA	1–2 year. Low power	30 mA. Low power	50 mA, very low power	30 mA low power
Range	Long range 10 km (Urban) 50 km (rural)	Short range 10–100 m	Short range 15–30 m	Short range 0–10 cm	Short range 15–30 m

So, maintaining security is a very crucial thing. In this section, we will discuss the attacks in the communication layer and defense mechanism.

For understanding security, three main terms need to know. First is attacker, who tries to access the device, data, and sometimes also tries to harm the device. There is another term that comes under Onion router, in which attacker makes themselves anonymous when they have to attack. The next term is defenders, who try to defend the system and devices by providing some defense mechanism. The last term is victim; this can be any device or person. As an attack can harm a device or person, an attack on the device such as a device is not able to access the resources, providing wrong information, and sending or receiving data from an unauthorized device.

The attacks in the IoT networks can harm not only the device but also the person. Such as, if a smart vehicle is attacked by an attacker, then it can set its speed, gear, and brake system in its hand. With this, he will be successful in damaging the vehicle, and this sort of attack can take the life of the person. In the smart home, the intruder can take the knowledge when no one is present at the home. In that situation, he will enter into the home and can steal things. There are smart weapons are also available which help in targeting the target with more accuracy. If an attacker can take control of these weapons, then it can take the life of an innocent person. This attacker can damage the system and can also be an obstacle to the growth of IoT.

At the communication level, attacks can be categorized into three types. Attack on topology, under this, three attacks occurs; sinkhole attack in which attacker introduced a wicked node in the network that node gives a bait details for routing. Through this, its neighbor nodes get attracted to updated routing details, and wicked nodes capture the data. The second attack is a wormhole, in which two malicious launched by the attacker at an appropriate position.

5.2.1 Sinkhole Attack

When data move from one node to another via a wireless network, the chances of an attack on this network will increase. The attack can be of two types such as internal attack and external attack. An internal attack, in which a member of the organization or network tries to attack and misuses the information, then it is known as an internal attack. The external attack was done by an attacker who is not to the organization (outsider of organization or network). A sinkhole attack is one of the internal attacks; in this, a malicious node enters the network. The attacker tries to launch a wicked node that advertises the best routing path to its neighbor. All neighbors find that path as a beneficial path and start sending their information via a new beneficial path. This makes all data firstly reach the wicked node then to its correct destination. After the entry of the wicked node, it updates the routing metric, and sometimes, it becomes difficult to predict this attack.

Researchers have given many defense mechanisms regarding sinkholes. In Jing et al. (2014), they have introduced a spy node that will present near to the source node then identify the malicious node in the network. The limitation of this scheme is that the spy node should be the neighbor of the source node, and that the malicious node is also a neighbor of the source node then only this scheme will work. In Aqeel-ur-Rehman et al. (2016), a dumpy packet is used by an extra node; this technique helps in identifying whether the packet is reaching its destination without any modification via the correct path. In Frustaci et al. (2017), uses a hop count method in which the base station (BS) updates its database with the hop count number. BS sends a packet to all nodes from it will calculate the number of hops it has taken to reach its destination. In this way, the wicked node that was representing its baited routing table will not work. An intrusion detection system for sinkhole is mentioned (Kibirige and Sanga 1505), where each node is monitored by the agent of attack detection. If any node finds out as a malicious node or on which attack has happened, then the agent communicates with other agents and updates the information. The intrusion detection system works in four phases, MDDR, *M* stands for monitoring each node; *D* stands for detection of malicious node; *D* stands for decision for malicious node, and *R* stands for the response for wicked node. Authors have approached the detection method; the defender tries to identify the group of malicious nodes and send information to the base station (Tabari et al. 2021). Nodes are more vulnerable in an open area and when sensors nodes are low powered. It is easy for the attacker to discharge these nodes. In a sinkhole attack, only, one wicked node can affect the whole network and changes the routing table for all nodes of the network.

The whole area of the network is divided into circles:

$$C_1,\ C_2,\ C_3,\ C_4 \ldots C_n$$

$$\text{The total area of network } = \sum_{i=1}^{n} C_1$$

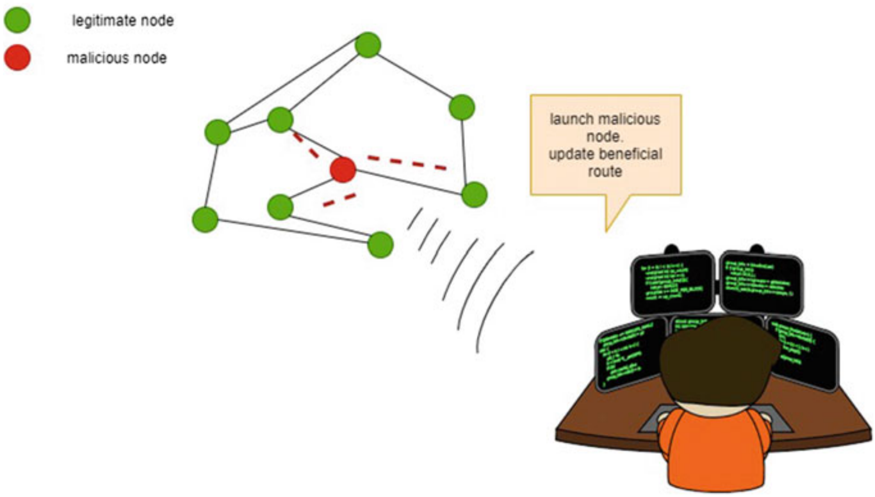


Fig. 5.9 Sinkhole attack

$$= \pi r_1^2 + \pi r_2^2 + \pi r_3^2 + \pi r_4^2 + \cdots \pi r_n^2$$

Let's take packet P_1 is sending from C_2 to C_7 with the route $C_2 \rightarrow C_5 \rightarrow C_6 \rightarrow C_7$.

Comparison of data*; if* $(C_2P_1! = C_5P_1! = C_6P_1! = C_7P_7)$.

Discard the packet P1;

Send acknowledgment to destination C7 that packet was modified by intruder;

So, the packet has been dropped (Fig. 5.9).

5.2.2 *Wormhole Attack*

Wormhole attack also comes under the attack on topology. In this, attacker launched two bad nodes at a position through which they can connect to the maximum neighbor. From which, they can large data or information. These two nodes make their way like a tunnel via it they share their information and update the neighboring routing table. In the updated routing table, each neighbor node finds that the tunnel way is more beneficial and starts sending information via a new way. In this way, the malicious node gets all confidential and any other information that is passing from them. Through this attacker can use, alter, and stop sending the information further. This attack is powerful as it can damage the network which has used encryption and decryption techniques. For measuring the impact of a wormhole attack, three terms come into the role. Wormhole nodes are nodes that come into the path from the root node to the malicious node. Global packet loss, in this, rate of loss of the packet by wormhole attack or by network both will be counted. Local packet loss, in this, is only about those packets which are lost due to neighbors of the malicious node. His attack affects the network in such a way that network will be cured after some time. It means that if the attacker removes his malicious node from the network, then the network shows some impact like packet loss rate may remain the same. Researchers have mentioned that not all neighboring nodes of the malicious nodes will lose the packets. There is the possibility that neighboring node follows their authentic routing path (Poovendran and Lazos 2007). Alenezi et al. (2021), a wormhole prevention method, *true_link,* works in two phases; the first phase is the connection phase; an *Request-To-Send* (RTS) is sent by the sender if it receives *Clear-To-Send* (CTS) in a threshold time, then it will proceed to the next phase. The next phase is the authentication phase, in which the sender authenticates the receiver and the receiver authenticates the sender. Both phases work in a strict timing environment. Through which, attackers will not be able to attack or alter the data. The predicted and actual timestamp will compare. If the value of the comparison is more than the fixed threshold value, then packet will be discarded. Wallgren et al. (2013), a light_weighted protocol, a guard node monitors the traffic across the network. This method does not require any other hardware specification as it is a resource-constrained environment. For authentication, it uses *pre_exchange_method*. Wormhole attack happens on routing protocol Chugh et al. (2012). The routing protocols are categorized into two types: periodic routing protocols and on-demand routing protocols. Periodic routing protocols in which, nodes update their routing table, whenever they found any change in its neighboring routing table. For this process, nodes use the distance-vector algorithm. On-demand routing protocol, nodes update their routing protocol only when a node wants to send information.

5.2.3 Black Hole Attack

Trending IoT network contains a huge number of nodes or devices. These devices are low powered, have low memory, and resource constraints in nature. These characteristics make them vulnerable to attack, and they cannot handle complex security because they have a limited amount of memory. So, attackers try different methods to access and harm the IoT devices. Black hole is also comes under the umbrella of attack; it has almost the same features as sinkhole and wormhole attacks. Black hole attack, this name comes from the black hole word that is related to the universe (Tamilselvan and Sankaranarayanan 2007). A black hole in-universe can absorb everything of the universe. Like this black hole attack works, as it absorbs all data traffic present in the network. In IoT network, nodes send data from one node to another with this update their routing table, and node selects the path that is beneficial to them or which has a low cost. So, in this attack, the attacker launches any number of malicious nodes. These bad nodes advertise themselves as they have containing the best route. From this bait route, nodes get attracted and start sending their data to bad nodes. These malicious nodes drop the packet. When correct destination will not be able to get the data, the node starts sending information, again and again; this makes a load on the network and harms the devices also. As devices are low powered, they start sending the same message, again and again; it consumes more power as expected. In respect of defending the network from this attack, time expiration and the sequence number have been used (Wazid et al. 2013). Time expires is not unique for all nodes as it depends on the number of hops it needs to take for reaching its destination. After sending a packet, if it does not get a reply in its time limit, then that route comes under a suspicious route. The node will send the next packet only when it gets a reply from the destination. An example of a black hole attack that degrades the performance of the network and decreases the throughput of the network system. Let take seven routers (R_1, R_2, R_3, R_4, R_5, R_6, R_7) are present and one coordinator (C_1). R_3 wants to send data to the coordinator of the network; for this, it takes route, $R_3 \rightarrow R_5 \rightarrow R_6 \rightarrow C_{1.}$ In this, R_5 is the node of a black hole, when data come to R_5, then it will not allow moving R_6. This way coordinator waits for the packet from R_3 and degrades the performance of the network. Prevention from this attack, an authentication mechanism is given. Clusters are made in the network, and each cluster has its coordinator, and the neighbor's coordinator can communicate among themselves. The coordinator sends an authentication packet to its nodes, and nodes reply with their identification number. If any node does not respond to the authentication packet, then the coordinator makes it a malicious node and discards that node. Mentioned a secure routing method named as BAAP algorithm in which it maintains a table of all authenticate nodes except this maintenance does not require any other additional resource (Wallgren et al. 2013).

5.2.4 Flood Attack

Communication in the IoT network, where different protocols are present for making reliable communication among the devices. Like this, attackers are present to make unreliable communication and give many impacts to IoT devices and their communication network. The attacker also makes an attack through which the user or node is not able to access resources; flood attack is one of these attacks. In this, the attacker sends a HELLO message to any particular or anyone number of nodes. He can also broadcast this HELLO message to the network. The attacker sends continuously HELLO messages to nodes, through which the authentic node or user will not be able to send or receive the correct information. From this attack, the energy consumption of nodes will also increase without doing any reliable work. When a node has less power, then it will not able to use some of the resources which require more power.

In a flood attack, a node acts as the legitimate node and copy the behavior of the authentic node. It starts sending messages to nodes. This attack can be stopped by setting the threshold value for several HELLO data packets within a time limit. If authentic nodes find that any node has crossed the value of threshold, then the node will be declared as a malicious node (Yan et al. 2018). Qureshi et al. (2020) use a machine learning algorithm for the detection of a flood attack, use the history of the node, and compare present routing information to the history routing information. Yan et al. (2018) use convolution neural network for detection of this attack. This attack is also known as the denial-of-service attack (DoS) (Perazzo et al. 2017). In this, attacker sends HELLO, SYN, RREQ packets to the node and tries to node not able to use resources. In (McDermott et al. 2018), authors have discussed the flood attack based on UDP. In this, a malicious node sends data (SYN, HELLO) packets to the node by using user datagram protocol (UDP), and the attacker uses an authentic source address for transmitting messages. The number of users of the Internet is increasing, and this is creating traffic and load on the network (Seth et al. 2020). Because of this traffic, the user would not be able to access the information from the Internet. So, there is a requirement of balancing and management of traffic. A cluster-based approach has been introduced in Palit et al. (2011). As we have seen, the site gets crashed when a large number of users try to access the same site simultaneously. If this same process is done by an attacker, then it is known as a flood attack. The attacker launched a virus in the targeted system and that virus does a flood attack on the system or HTTP-GET attack on a particular website. For preventing this type of flood attack, nodes check the pattern of accessing the Web site; if the node finds it as a flood attack, then it will block that IP address from which it gets HTTP-GET messages in a flooded manner (Fig. 5.10).

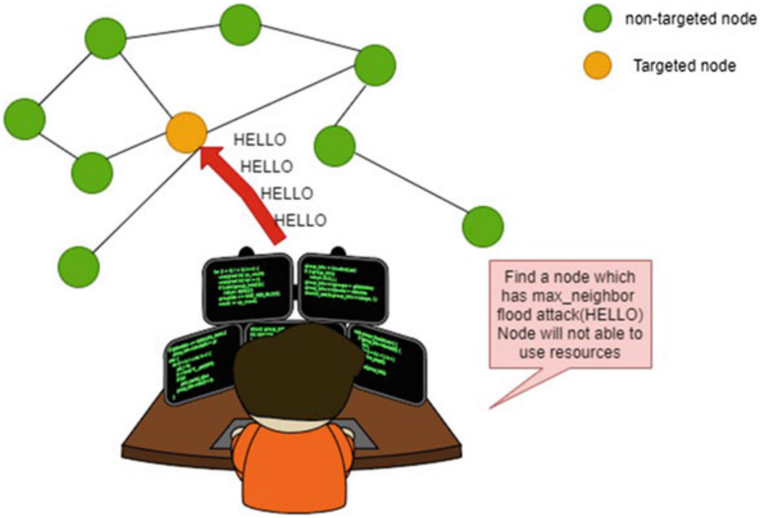

● non-targeted node
● Targeted node
HELLO
HELLO
HELLO
HELLO
Find a node which has max_neighbor flood attack(HELLO) Node will not able to use resources

Fig. 5.10 Flood attack

5.2.5 Rank Attack

In the communication layer of IoT architecture, there is a requirement of routing protocol (RPL). RPL is a very crucial part of reliable communication among nodes. In this, nodes are arranged in DODAG form. The acronym of DODAG is destination-oriented directed acyclic graph. It follows the ICMPv6 protocol for the control message. Under the umbrella of the control message, four DIO is used for containing the information about nodes, and it helps in identifying the required node. DIS is used when a new node enters the network and advertises its information. DAO, its task is to provide the route from root to destination node. The root node contains all information about the routing metric. DAO-ACK is a way of saying that node has received the data. So, it sends an acknowledgment packet to the source node. In RPL, each level of the graph has ranked in ascending order from root to node. Each node is connected to many nodes, and for each node, it can calculate its best path, or it can also use a multi-hop path for sending information. When a node receives a message from a lower-rank node, then the node understands that message has come from the parent node. One of the attacks on RPL is a rank attack; in this, attacker launched a node with fake information (low-rank value). A malicious node enters the network and gets a connection to its neighbor nodes. When neighbor nodes identify that a malicious node has a low-rank value, then they make it as their parent node and start sending information to the malicious node, and with this, they also update their rank value. By updating their rank value, whole network gets disrupted because each node gets to start to update their rank value. In (Limbasiya and Karati 2018), if there is a bad change in the packet delivery mechanism, then it can degrade the performance of the network by 60%. This attack is known as a decreased rank attack. Attackers also use the increased rank attack method. This attacker either can increase the rank of any node or launch a new bad node with a higher rank or get connected to its neighbor. When all the neighboring node finds increased rank value node, then they start changing their parent node. This attack will use more resources like changing parent node, and changing one's rank value uses energy consumption. In this way, the attacker can attack resources and degrade the performance of the network.

5.2.6 Cryptanalytic Attack

Cryptanalytic attack in which attackers try to capture the data that are traveling in the network, when the attacker gets this data tries to decode the encrypted data. In this attack, the attacker can drop, change the route, and alter the data. Man-in-middle also comes under this attack. The attacker comes into the legitimate network and takes data from an authentic sender. After capturing the data, he will modify it or try to access the crypto-algorithm or key for decoding the data. Then, he sends information to an authentic destination. The attacker also captures the data that are sent by the receiver such as acknowledgment or reply of information. The attacker modifies that data also and sends it to its destination. In this way, source and destination assume that data are reaching its correct location and data are coming from authentic location, respectively. This attack can occur in any layer of IoT architecture.

A Vigenere cipher has been used, and a genetic algorithm is used for breaking the cipher (Lee et al. 2014). In the Vigenère cipher, a table has maintained all alphabets with their index number, and a keyword is used. A keyword is repeated till the size of plaintext. As a result, ciphertext comes after adding a keyword index with plaintext index; the resultant of these indexes comes up with cipher alphabet. Knapsack cipher has been used for security, and this is broken by genetic algorithm. Crypt analytical attack on the RSA algorithm is used in the network (Rao and Prema 2019).

Recent Attacks in Communication of IoT Network

IoT network contains a large amount of data which makes it attractive to the attacker for attack and accessing the information. Attack on smart electric vehicle charger is done by the attacker (Alladi et al. 2020). By changing the authentication mechanism, attacker can enter into the system via wrong password. The attacker changes the details of the vehicle and set of current usage. From this, we analyzed those attackers focused on non-authentication communication. In another attack on a smart meter, the attacker used the smart meter_id and access the system (Alladi et al. 2020). From this, he was able to modify the meter reading value. In Shadon, many DLink Web cameras are installed. They are directly connected to the Internet and cloud services (Seralathan et al. 2018). Attackers hack the Web camera and access it remotely. This was done because cameras were installed with an administrative password. Smart plugs (Ling et al. 2017) of brand Edimax are also vulnerable to attack and provide insecure communication. These plugs were mostly installed at home and in shops. In this, the attacker focused on destroying the communication protocols. The main weakness of these smart plugs was limited to 4-digit passwords and limitless attempts for entering the password.

Nowadays, voice assistant IoT devices are in demand. Amazon Alexa is one of the most popular voices assistant devices. In a case study of the attack of the Amazon Alexa (Lei et al. 1712), two attacks were done on the device. One is a fake order, and the other one is opening the door of the house. For entering into the house, there is a requirement of managing the key of the lock. For this, smart lock came into view; these locks keep the record of the opening and closing of the door. August smart locks are vulnerable to attack (Ye et al. 2017). The attacker enters the owner's account and uses the account. From this, he also gets the personal information of the owner. For this attack, the attacker used the Bluetooth jammer and rooted mobile phone; these exploit the communication between owner and smart lock.

Distributed denial-of-service (DDoS) attack is a very common attack on IoT devices. There is a type of DDoS is reflection attack. Simon et al. have presented a case study on this attack. This attack is based on the traffic in communication among the devices. IP camera Airlive has taken for the attack (Maity et al. 2022). On this, UDP packets were sent every 50 microseconds. From this, IP camera sent an error message and was unable to work its main task. Hence, we have analyzed that security issues are also increasing with the growth of IoT devices. Thus, there is a requirement for a defense mechanism against the security issues on the communication among devices. In the next section, we have mentioned some defense mechanisms.

5.3 Defense Mechanism

IoT network is surrounded by three terms conventional and comfortable life, issues, and its defense mechanism. This network is much prone to attack due to the less involvement of human beings and its autonomous nature. This is one of the reasons for cyber-attack. Other reasons are components in IoT networks are low powered and have low storage, so it is difficult for the components to handle complex security structure or complex cryptography. The components are connected via a wireless network, which is one positive point for an attacker to access the data from devices. Attackers can damage devices or components, steal information, alter the information, and be an obstacle in service provided by IoT devices to the end users. Two important aspects for maintaining security are authorization of device and person or any entity of network, and with this, access control is also important. For enhancing the IoT network, security is on the top. To maintain this, there is the requirement of a sequence of knowledge about this network as shown in Fig. 5.11. The first thing to know is about all the components that are used in a network with their function and working. The next thing about the vulnerability of components can be broken into two types' hardware vulnerability and software vulnerability. To know about, hardware vulnerability is a strenuous effort. On the other side, software vulnerability can be found in the operating system (Nucleus RTOS, Tizen, TinyOS, Apache Mynewt) used in the network, in communication protocols, and in device drivers. After knowing the components and vulnerabilities, we have to go on different types of attacks and have knowledge of how attacks are happening. Afterward, a defense mechanism comes into its role. In this section, we will discuss different defense mechanisms in the communication layer of IoT architecture.

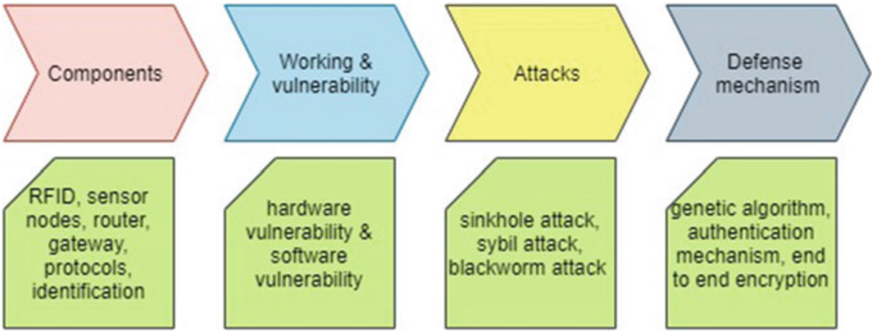

Components
Working & vulnerability
Attacks
Defense mechanism
RFID, sensor nodes, router, gateway, protocols, identification
hardware vulnerability & software vulnerability
sinkhole attack, sybil attack, blackworm attack
genetic algorithm, authentication mechanism, end to end encryption

Fig. 5.11 Steps to reach at defense mechanism

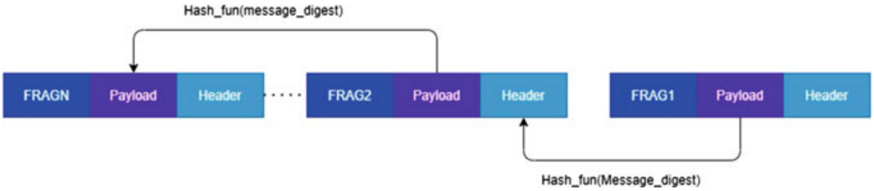


Fig. 5.12 Content chaining

5.3.1 Content Chaining Scheme

As we know, components used in IoT networks are low-powered devices and resource constrained in their behavior. So, managing security with these characteristics is difficult. Attackers try different techniques to enter into the network or capture data or harm the device/components used in the IoT network. The network also tries to maintain security with the help of using a pair of keys. These keys are stored and controlled by a controlled certified authority. This will help only authenticated nodes help in transferring messages. But, sometimes, attacker tries to access the key, and using some techniques, he will be able to get access to the network. After entering into the network, it gives a fake node that sends the messages in a flooding fashion. Because of this, device will not be able to use resources. The gateway can use a defense mechanism that helps to identify which node is getting overloaded. From this, it can identify that an overloaded node can be an attacker's node.

In communication, layer packets can be fragmented into many fragments. It uses a token to reassemble before reaching to next layer. It also uses a timer for taking quick action if data drop or reach the wrong destination. Sometimes, attackers send duplicate fragments for making a disturbance in network and using more energy. For this, node can check the MAC address of the source node. It can also use the content chaining method. This packet is divided into different fragments that store two important sections payload and header. The first fragment (FRAG1) stores all the routing information, and from its payload, a digest will be taken. After taking the digest of payload, a hash function is applied to it. The value of the hash function will store in the next fragment (FRAG2) with this token value also stored in the header of FRAG2. This process will continue till the last fragment as shown in Fig. 5.12. So, if the attacker tries to break this chain, destination node easily identifies that fake data have come to its place.

5.3.2 Authentication Defense Mechanism

Authentication is a major part of maintaining security. It helps in identifying the authentic nodes and this can be done by RFID, EPC, 6LoWPAN, and many other protocols are present for unique identification of nodes. Even these protocols get the access to enter into the network. Management of key is also used in authentication of devices. A central controller authority (CCA) is used for providing keys. Symmetric key encryption method can be used in which the same key is used by both nodes for encryption and decryption of the information. This is maintained by CCA. Asymmetric key encryption method can also be used in which combination of the public and private key used by nodes. This is also managed by CCA. CCA can also provide a one-time session key for providing the authentication mechanism.

Another method that can be used for authentication is node should know the data rate of the communication protocol that has been used in the network. There are limited packets allowed to send on a particular path. From this information, a node can calculate how much time a packet takes to reach its destination and receive the acknowledgment of the packet. If the node finds timestamp value is greater than the expected, then it will be discarded by the node. A threshold value of payload should be set if a node finds payload value of packet greater than the threshold value, then also it will be discarded by the node.

Authentication of nodes can be maintained by using passwords against the node. If password protection is a single layer, then devices are vulnerable to attack. Kim and Lee (2017) in this, researchers have proposed a secure vault for providing a secure system. In this, they have used a three-layered password protection mechanism. This method is started by the client; the client sends the first layer password to the server of the network. Then, the server sends a challenge for authentication and checking source is legitimate or not. Then, the sender sends the response of challenge; if the receiver finds it as a valid response, then the receiver approves the sender as a legitimate sender. Uses a two-step authentication mechanism, first step is the setup phase in which the node sends its identity number and asks for registration (Mahmood et al. 2016). The second step is the authentication phase; the sender asks for a one-time password with a request message in which it includes its registration number (Saxena et al. 2014), machine learning authentication scheme based on hypothesis testing. Biometric and behavioral authentication mechanism is used (Li and Zhang 2019). Biometric authentication methods include such as fingerprint face recognition, iris scan, electrocardiogram, ear shape, and many others. Behavioral authentication mechanism includes such as keystroke, hand gestures, voice recognition, signature, and recognition. OAuth uses for authentication for devices (Khraisat and Alazab 2021).

5.3.3 Intrusion Detection System (IDS)

Intrusion detection system term comes from the term intruder, who tries to access the network and data that are transmitted from one device to another. For the detection of activities of intruders, an intrusion detection system has comes up. The intruder can enter into the network and does the malicious activity, or he can do it even from outside of the network. IDS’ main task is to detect where the malicious has been done and give warning and alarm to the legitimate node for attack done by the intruder.

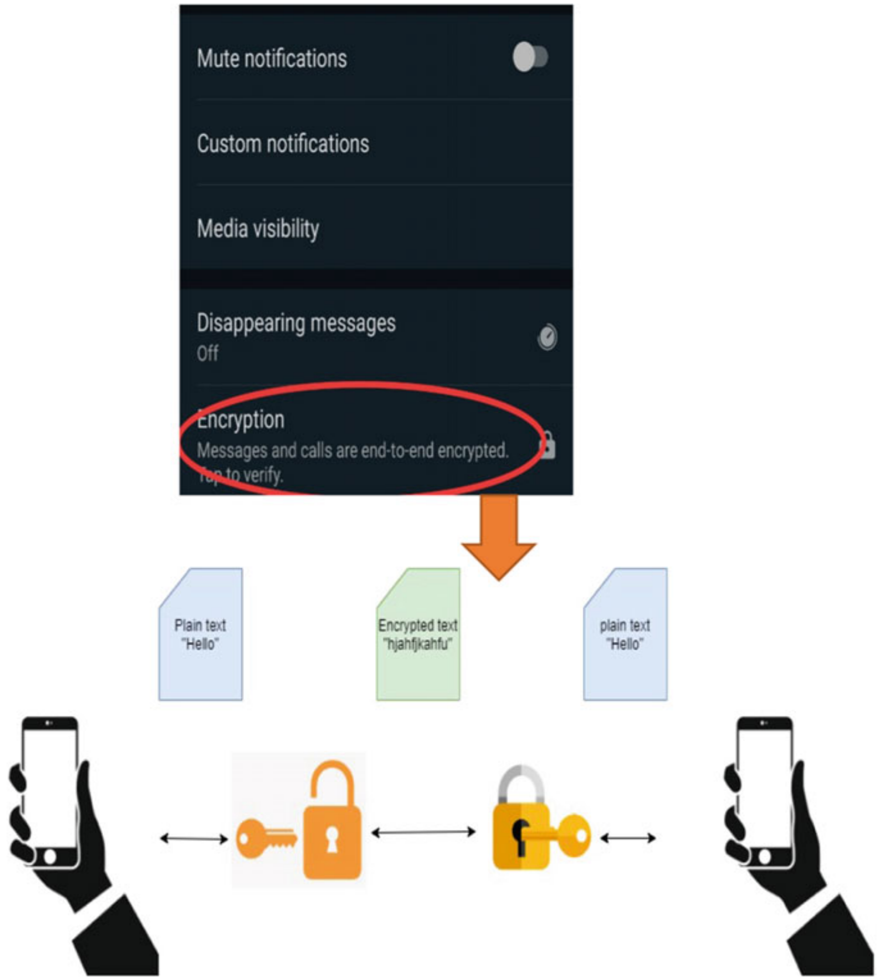
This system keeps an eye on the network and nodes; if any node sends data in a flooded manner, then it will detect it as a malicious node. In simple terms, IDS helps in analyzing the network on which basis it finds about the malicious node.

IDS can be done by signature- or pattern-matching method; in this method, it makes a database that stores the signature of nodes. When the node transfers message from one to another node, then IDS system will check whether the packet has the same signature as the node or not. This analyzing process will be done by checking from the database. Creating a database requires memory, so this is one disadvantage with signature-based IDS. It also requires time to time updates. If any new legitimate node enters the system, then its signature should be updated in the database. For using it efficiently, this system should be dynamic; otherwise, it can drop the legitimate packet. Another method of IDS is based on finding anomalies in the network. In this, it tries to find any abnormal activity in the network with the help of statistics. An anomaly system identifies if any link or node is overloaded in the network. Then, it will try to analyze the reason behind overloading. This approach is better than the signature system as it does not require updating. This system works efficiently in a static manner.

The intrusion detection system can use a machine learning classifier to classify the packets into a normal packet or abnormal packet (Santos et al. 2021). The packet-count approach is used based on the sliding window method (Nimbalkar and Kshirsagar 2021). Two methodologies used pattern-based intrusion detection systems and anomaly-based intrusion detection systems (Kalnoor and Gowrishankar 2021). State transition diagram has been used for the intrusion detection system (Lizardo et al. 2021). Kan et al. (2021), a hybrid approach for the intrusion detection system. In this approach, two machine learning algorithms have been used: *support_vector_machine* and *decision_tree.*

5.3.4 End to the End Encryption Method

End-to-end encryption method helps in protecting confidential data from intruders. In this method, encryption is done on the sender side, and decryption is done on the receiver side. In sending information, a third party can also involve and help in storing data. But, it can store only encrypted data. This means that a third party will not be able to see what data have been sent. This encryption method is also available in WhatsApp as shown in Fig. 5.13. In this app, we send messages to another person. This encryption method encrypts data at our side and decrypts only the receiver side. In this case, our data are safe from the attacker. But, sometimes, this method also faces some challenges and issues such as man-in-middle attack can occur in this method. An attacker acts as a legitimate sender and receiver; through this, it receives data and key also. After getting the key, it can also analyze the encryption and decryption method. An encrypted online chat system has been introduced by using the RSA algorithm for encryption and decryption along with the digital signature (Mahmood et al. 2016).



Mute notifications

Custom notifications

Media visibility

Disappearing messages
Off

Encryption
Messages and calls are end-to-end encrypted. Tap to verify.

Fig. 5.13 End-to-end encryption in WhatsApp

5.4 Network Optimization Techniques

Network optimization is one of the terms that is gaining importance in the field of IoT because of the exponential growth of the application of the IoT. They are producing a certain amount of data, and integration of this data becomes huge data. And this will increase the load and traffic of data in the IoT network. This traffic gives an impact on the efficiency of the network which will degrade the performance of the network. These issues can decrease the exponential growth of IoT networks. For maintaining the growth, there is a requirement to optimize the network so that it gives an optimized result. It will also help in sending data at a higher rate if there is proper optimization

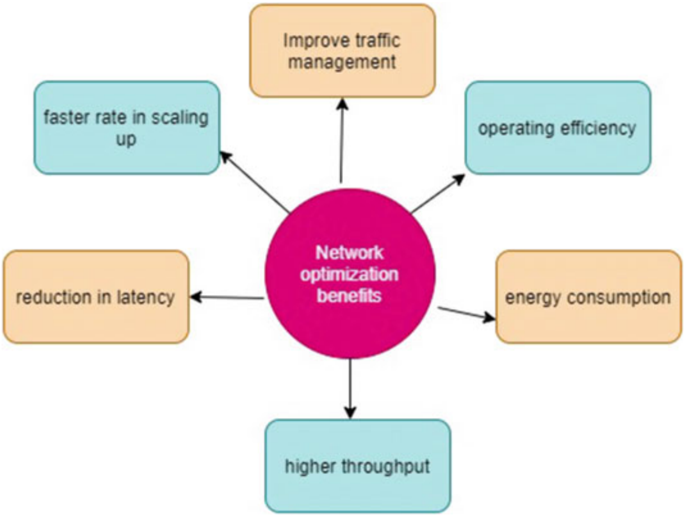

Improve traffic management
faster rate in scaling up
operating efficiency
Network optimization benefits
reduction in latency
energy consumption
higher throughput

Fig. 5.14 Benefits of network optimization

techniques used in the network. Network optimization techniques give us benefit in several ways such as it helps in managing the traffic of the network; if it helps in maintaining a balance of network, then its operating rate will also be efficient. This way IoT network will consume fewer resources and become an energy-efficient network. It also helps in giving higher throughput. Network optimization can be done by using an old algorithm or by using a new novel algorithm. But, sometimes, network optimization becomes a complex problem; then, a mixture of the old and novel algorithms will help to solve the issue. In this section, we will discuss some algorithms that help in network optimization (Fig. 5.14).

5.4.1 Particle Swarm Optimization (PSO)

Particle swarm optimization term has come from the nature of swarm. It is one of the computational techniques which helps in solving the problem and optimizing it. This swarm produces particles that move in search space area and try to find an optimized path. After finding the path, it tells to swarm. The same approach uses in optimizing the network. In Liu et al. (2021), researchers have proposed an algorithm based on PSO that uses the orthogonal computational learning strategy. In this algorithm, they have used a sink node that is movable and helps to identify and repair the routing path. In the result of this algorithm, it was proved in decreasing the overhead of the network, and this also helps in reducing the usage of energy. In Cao et al. (2021), authors try to analyze the power consumption of nodes with the help of making clusters in the network. In clusters, they have used the PSO scheme, and it helps in saving energy for each node, as each node needs not compare with all nodes. In a cluster, nodes will compare only in their cluster and save energy. In this scheme, one limitation is present as making ahead in the cluster is bit energy consumption process. In Saxena et al. (2015), researchers have combined quantum computing with PSO that helps in giving a better result in searching and also helps in fast convergence results. In this scheme, they have also given network optimization with a better approach of selection of the cluster head. They used an improved version of PSO in which they have tried to reduce the noise disturbance and redundant data. A broker was introduced between the cloud server and IoT network; this broker helps in reducing the response time of the node (Nandan et al. 2021).

5.4.2 Genetic Algorithm (GA)

A genetic algorithm tries to find the fittest for surviving in different conditions and for producing offspring. This algorithm is based on the evolution of nature. Uses cluster technique and GA, in this, nodes present in the network make some clusters, and GA helps in identifying a beneficial path, with the help of length of the path and residual energy of node (Alshamrani and Basha 2021). As a result of this scheme, save energy, increase the throughput of the network, and helps in optimizing the network. A constrained environment was considered. In this, node uses the CoRE interface which the CoRE interfaces which use a smaller number of control messages. CoRE interface scheme helps in using the energy efficiently. Authors have mentioned using GA in searching for the node which has more storage and more energy. That node will be annotated for finding the best route for the transmission of messages (Janarthanan et al. 2021).

Authors have used the GA algorithm for network optimization. Numbers of clusters are made in a network. In each cluster, one head was selected (Tipantuña and Hesselbach 2021). Each cluster will be directly connected. The main challenge in this approach is finding a cluster head, which helps in optimizing the network. For this, crossover, mutation, and fitness techniques are used. If two nodes have the same fitness value, then the minimum fitness value of their network will be deleted. And the important thing, they have observed is that for making a cluster head, distance is an important aspect (Fig. 5.15).

5.4.3 Heuristic Algorithm

A heuristic algorithm is made for solving difficult and compounded problems in a very efficient manner. It also helps in solving the problem in an easier and faster way from which it can give an optimal solution. In the network, it is very obvious that redundant and some partial data make the load on the transmission link. The heuristic algorithm helps in identifying the redundant data and dropping that packet by which it optimizes

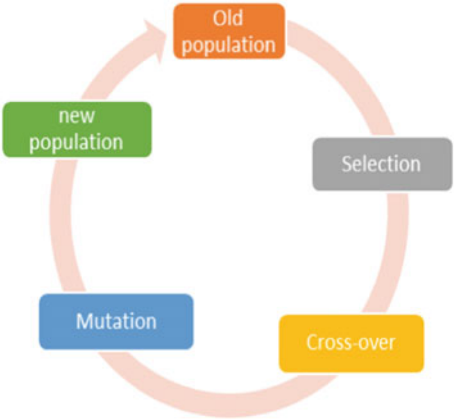


Fig. 5.15 Cycle of genetic algorithm

the network. In Patra et al. (2021), authors have proposed the routing protocol based on the heuristic algorithm; this protocol uses the shortest path for transmitting data from one node to another node. It identifies the path based on characteristics of the link such as data rate and distance between nodes. In Yadav (2021), researchers proposed a novel algorithm that helps in making an energy-efficient network. This algorithm switches data from device to smart device.

5.5 Challenges in Network Optimization

IoT has given us many applications in almost every sector such as in industry, health, education, environment, home, cities, rural, parking, and many others. All components under these applications do communicate with the help of different protocols. In protocols, they used different topologies for transmitting the data. Most of the protocols are based on IEEE 802.15.4 standard and use mesh topology. Making efficient communication among devices via using mesh topology is a difficult task and challenge of network optimization. In this section, we will discuss the different challenges for optimizing a network.

(1) Routing

Communication protocols use different topologies for sending information such as mesh topology, star topology, and some are based on cluster method. For routing in network, it has to maintain a routing table. When a new node wants to join the network, then the routing table should be updated. It also means that table should be dynamic. This is one of the challenges of network optimization. Some routing protocols make non-root nodes overloaded with the whole network routing information. Because of this overhead, it gives challenge in network optimization. Protocols that used cluster method for transmitting the message, in this making, a cluster head is also one of the overheads.

Problems:

- Need of energy-efficient routing protocols for the network.
- A dynamic routing database requires for reliable network.
- Routing algorithm which has less overhead for sending messages.

(2) Mobility

IoT is not about only static nodes, it also includes mobile nodes. These nodes create an overhead of maintaining information about these nodes. These nodes also change their subnet IP address and are mobile nodes. When a node moves from one network domain to another network domain then there is a need for the best route for making an energy-efficient network. This gives a challenge for changing the information of the node.

Problems:

- Proper maintenance of all nodes which are moving from one place to another.
- Authenticate a new node if it is entering from the outside network with less overhead.

(3) Multicast

Multicast is used when a node wants to send information to any number of nodes. Some protocols fell asleep after sending a message to many number nodes. In this method, if data do not reach its destination before falling asleep, then data will drop. Another issue in multicasting is some protocols do not give acknowledgment about the multicast packet. In this way, the source node will not be able to identify whether the packet has reached or not.

Problems:

- Proper sleep and awake method for nodes.
- Sometimes, packets can be lost because of their dormant state.

(4) Security

Security is a major concern of all architectural layers of IoT. The communication layer which handles most of the work of networking also suffers from the challenge of maintaining security. Security is one of the things that helps in increasing the productivity of IoT devices. As it carries a huge amount of data that also includes some confidential data, for this reason, security is very important. In the communication layer, security is important because an attacker can remove the node of the network, can add the malicious node, and can alter the information of the node.

Problems:

- A security mechanism with less overhead.
- A security method should be updated from time to time.
- Improve the weakness of the security method of the network.

(5) Heterogeneity

IoT network is made up of integration of the different networks. These networks can have different characteristics such as medium of data transfer, security, data rate, frame size, and many others. Managing this integration of the network is a complex and difficult task. This also takes the consumption of energy and resource management to become difficult as a comparison to a homogenous network.

Problems:

- An energy-efficient method for different applications.
- Management of resources for all heterogenic nodes.

(6) Scalability

IoT devices are increasing with a very high pace due to this, managing all connections among the devices is challenging. In an IoT network, sometimes, an anonymous node wants to enter into the network. And load balance among different networks is also a challenge. These challenges make an obstacle in the optimization of the network.

Problems:

- Management of resources for all nodes inefficient manner.
- Require a load balance method with an efficient technique.

5.6 Conclusion and Future Direction

We can conclude the chapter as IoT began with the Internet and communication among devices. Now, this connection among devices is getting complex day by day. Researchers have already provided a lot of protocols for communication, and their issues and challenges are also available. These protocols are chosen according to the application and need of devices. In this chapter, we have discussed some of the communication protocols that help in transferring the message from one application to another. Some protocols help in transferring information in a very long distance, and some require being in contact of a few meters. A comparison of these protocols is useful to researchers for further study and making new protocols for communication. New technology can not come without any issues like this; IoT has also come with many issues and challenges. In this chapter, we have discussed the different attacks in the communication layer of IoT and also mentioned the defense mechanism of attacks. The motivation for choosing attacks is that security is the topmost issue in IoT. In the last section of this chapter, we have given a review of the optimization of the network. In this, the importance of network optimization is mentioned. This chapter will help the researcher to know about the communication layer of IoT.

With the advancement of IoT technology, the number of IoT devices is increasing. Management of this huge network and data produced by this network is a complex task. In this sub-section, we have mentioned future direction, and this section helps in finding direction. *Heterogeneity* of IoT network, components of network do communicate among them using different communication protocols in the same network. Maintaining this network becomes a difficult task nowadays; it is necessary to make the network an efficient network. From starting of the Internet and the Internet of Things, *Security* remains a direction for research. IoT devices produced a huge amount of data with the inclusion of confidential information. *Mobility* of nodes, modern IoT devices are mobile; they change location from one place to another. The nature of mobility of the IoT devices becomes a difficult task as a network has to maintain a dynamic record or database for devices and components of IoT. *Big data* are also a direction for research. As with the increment of the number of IoT devices, data producing by these devices is also tremendous. Storing this tremendous data using cloud storage is still a challenging task. *Energy-efficient* components of IoT are low powered and resource constrained. So, there is the requirement of maintaining an energy-efficient system and network that uses less resource and low power.

References

Aju OG (2015) A survey of zigbee wireless sensor network technology: topology, applications and challenges. Int J Comput Appl 130(9):47–55

Alenezi FAF, Song S, Choi B-Y (2021) WAND: wormhole attack analysis using the neighbor discovery for software-defined heterogeneous internet of things. In: 2021 IEEE international conference on communications workshops (ICC Workshops). IEEE

Al-Kashoash HAA et al (2019) Congestion control in wireless sensor and 6LoWPAN networks: toward the Internet of Things. Wirel Netw 25(8):4493–4522

Alladi T et al (2020) Consumer IoT: security vulnerability case studies and solutions. IEEE Consum Electron Mag 9(2):17–25

Alshamrani SS, Basha AmjathFareeth (2021) IoT data security with DNA-genetic algorithm using blockchain technology. Int J Comput Appl Technol 65(2):150–159

Alharthi S, Johnson P, Randles M (2020) Secure and energy-efficient communication in IoT/CPS. Recent Trend Commun Netw

Aqeel-ur-Rehman SUR et al (2016) Security and privacy issues in IoT. Int J Commun Netw Inform Secur (IJCNIS) 8(3):147–157

Cao WL, Kang LL, Liu Z-W (2021) Dual-drive opposition-based non-inertial particle swarm optimization for deep learning in IoTs. J Supercomput 1–15

Cheng Y-K, Chang RY (2017) Device-free indoor people counting using Wi-Fi channel state information for Internet of Things. In: GLOBECOM 2017–2017 IEEE global communications conference. IEEE

Chugh K, Aboubaker L, Loo J (2012) Case study of a black hole attack on LoWPAN-RPL. In: Proceedings of the sixth international conference on emerging security information, systems and technologies (SECURWARE), Rome, Italy (August 2012)

Dizdarević J et al (2019) A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Comput Surv (CSUR) 51(6):1–29

Dominikus S, Aigner M (2007) mCoupons: an application for near field communication (NFC). In: 21st international conference on advanced information networking and applications workshops (AINAW'07), vol 2. IEEE

Frustaci M et al (2017) Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet of Things J 5(4):2483–2495

Gentili M, Sannino R, Petracca M (2016) Bluevoice: voice communications over bluetooth low energy in the internet of things scenario. Comput Commun 89:51–59

Gonzales YI (2012) Application of near field communication technology for mobile airline ticketing. J Comput Sci 8(8):1235–1243

Gonzalez GR, Organero MM, Kloos CD (2008) Early infrastructure of an internet of things in spaces for learning. In: 2008 eighth IEEE international conference on advanced learning technologies. IEEE

Hortelano D et al (2017) From sensor networks to internet of things. Bluetooth low energy, a standard for this evolution. Sensors 17(2):372

Janarthanan N, Vasantha Kumar J, Balamurugan S (2021) IoT and genetic algorithm based automated central controller for effective congestion management in power system. In: 2021 IEEE second international conference on control, measurement and instrumentation (CMI). IEEE

Jing Q et al (2014) Security of the Internet of Things: perspectives and challenges. Wirel Netw 20(8):2481–2501

Kalnoor G, Gowrishankar S (2021) Intelligent system for intrusion detection in internet of things-wireless sensor network (IoT-WSN) smart environment

Kan X et al (2021) A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network. Inform Sci 568(2021):147–162

Khraisat A, Alazab A (2021) A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity 4(1):1–27

Kibirige GW, Sanga C (2015) A survey on detection of sinkhole attack in wireless sensor network. arXiv preprint arXiv:1505.01941

Kim H, Lee EA (2017) Authentication and authorization for the Internet of Things. IT Professional 19(5):27–33

Lee J-Y, Lin W-C, Huang Y-H (2014) A lightweight authentication protocol for internet of things. In: 2014 international symposium on next-generation electronics (ISNE). IEEE

Lei X et al (2017) The insecurity of home digital voice assistants—Amazon Alexa as a case study. arXiv preprint arXiv:1712.03327

Li P, Zhang Y (2019) A novel intrusion detection method for internet of things. In: 2019 Chinese control and decision conference (CCDC). IEEE

Li L et al (2011) The applications of wifi-based wireless sensor network in internet of things and smart grid. In: 2011 6th IEEE conference on industrial electronics and applications. IEEE

Li Y et al (2018) Passive-zigbee: enabling zigbee communication in iot networks with 1000x+ less power consumption. In: Proceedings of the 16th ACM conference on embedded networked sensor systems

Limbasiya T, Karati A (2018) Cryptanalysis and improvement of a mutual user authentication scheme for the Internet of Things. In: 2018 international conference on information networking (ICOIN). IEEE

Ling Z et al (2017) Security vulnerabilities of internet of things: a case study of the smart plug system. IEEE Internet of Things J 4(6):1899–1909

Liu J et al (2021) Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access 9:38254–38268

Lizardo A et al (2021) End-to-end secure group communication for the Internet of Things. J Inform Secur Appl 58(2021):102772

Mackensen E, Lai M, Wendt TM (2012) Bluetooth low energy (BLE) based wireless sensors. Sensors. IEEE

Mahmood Z, Ning H, Ghafoor AU (2016) Lightweight two-level session key management for end user authentication in Internet of Things. In: 2016 IEEE international conference on internet of things (iThings) and IEEE Green computing and communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE

Maity P, Saxena S, Srivastava S, Sahoo KS, Pradhan AK, Kumar N (2022) An effective probabilistic technique for DDoS detection in OpenFlow controller. IEEE Syst J. https://doi.org/10.1109/JSYST.2021.3110948

McDermott CD, Majdani F, Petrovski AV (2018) Botnet detection in the internet of things using deep learning approaches. In: 2018 international joint conference on neural networks (IJCNN). IEEE

Nandan AS, Singh S, Awasthi LK (2021) An efficient cluster head election based on optimized genetic algorithm for movable sinks in IoT enabled HWSNs. Appl Soft Comput 107:107318

Nieminen J et al (2014) Networking solutions for connecting bluetooth low energy enabled machines to the internet of things. IEEE Netw 28(6):83–90

Nimbalkar P, Kshirsagar D (2021) Feature selection for intrusion detection system in Internet-of-Things (IoT). ICT Express 7(2):177–181

Palit S et al (2011) A cryptanalytic attack on the knapsack cryptosystem using binary firefly algorithm. In: 2011 2nd international conference on computer and communication technology (ICCCT-2011). IEEE

Patra SS et al (2021) Meta-heuristic algorithms for best IoT cloud service platform selection. Integr Cloud Comput Internet of Things: Found Anal Appl 299–318

Perazzo et al (2017) DIO suppression attack against routing in the Internet of Things. IEEE Commun Lett 21(11):2524–2527

Poovendran R, Lazos L (2007) A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Netw 13(1):27–59

Qureshi KN et al (2020) A novel and secure attacks detection framework for smart cities industrial internet of things. Sustain Cities Soc 61:102343

Ramya CM, Shanmugaraj M, Prabakaran R (2011) Study on ZigBee technology. In: 2011 3rd international conference on electronics computer technology, vol 6. IEEE

Rao V, Prema KV (2019) Light-weight hashing method for user authentication in Internet-of-Things. Ad Hoc Netw 89:97–106

Rashid MA, Han X (2016) Gesture control of ZigBee connected smart home Internet of Things. In: 2016 5th international conference on informatics, electronics and vision (ICIEV). IEEE

Ribeiro GGL et al (2018) An outdoor localization system based on SigFox. In: 2018 IEEE 87th vehicular technology conference (VTC Spring). IEEE

Safaric S, Malaric K (2006) ZigBee wireless standard. In: Proceedings ELMAR 2006. IEEE (2006)

Santos L et al (2021) A flow-based intrusion detection framework for internet of things networks. Cluster Comput (2021):1–21

Saxena S, Sanyal G, Sharma S, Yadav SK (2015) A new workflow model for energy efficient cloud tasks scheduling architecture. Second Int Conf Adv Comput Commun Eng 2015:21–27. https://doi.org/10.1109/ICACCE.2015.139

Saxena S, Sanyal G, Srivastava S (2014) Mutual authentication protocol using identity-based shared secret key in cloud environments. In: International conference on recent advances and innovations in engineering (ICRAIE-2014), pp 1–6. https://doi.org/10.1109/ICRAIE.2014.6909267

Seralathan Y et al (2018) IoT security vulnerability: a case study of a web camera. In: 2018 20th international conference on advanced communication technology (ICACT). IEEE

Seth AD, Biswas S, Dhar AK (2020) Detection and verification of decreased rank attack using round-trip times in RPL-based 6LoWPAN networks. In: 2020 IEEE international conference on advanced networks and telecommunications systems (ANTS). IEEE

Sidna J et al (2020) Analysis and evaluation of communication protocols for IoT applications. In: Proceedings of the 13th international conference on intelligent systems: theories and applications

Tamilselvan L, Sankaranarayanan V (2007) Prevention of blackhole attack in MANET. In: The 2nd international conference on wireless broadband and ultra wideband communications (AusWireless 2007). IEEE

Tipantuña C, Hesselbach X (2021) IoT-enabled proposal for adaptive self-powered renewable energy management in home systems. IEEE Access 9:64808–64827

Venkatesh A et al (2017) A food monitoring system based on bluetooth low energy and Internet of Things. Int J Eng Res Appl 7(3):30–34

Wallgren L, Raza S, Voigt T (2013) Routing attacks and countermeasures in the RPL-based internet of things. Int J Distrib Sens Netw 9(8):794326

Wazid M et al (2013) Detection and prevention mechanism for blackhole attack in wireless sensor network. In: 2013 international conference on communication and signal processing. IEEE

Yadav R (2021) ADAS authentic data allowed security in internet of things. Turkish J Comput Math Educ (TURCOMAT) 12(13):1761–1765

Yadollahzadeh Tabari M, Mataji Z (2021) Detecting sinkhole attack in rpl-based internet of things routing protocol. J AI Data Min 9(1):73–85

Yan Q et al (2018) A multi-level DDoS mitigation framework for the industrial Internet of Things. IEEE Commun Mag 56(2):30–36

Ye M et al (2017) Security analysis of Internet-of-Things: a case study of august smart lock. In: 2017 IEEE conference on computer communications workshops (INFOCOM WKSHPS). IEEE

Chapter 6
Intrusion Detection System with Layered Approach to Internet of Things—A Business Paradigm

Sunil Gupta, Goldie Gabrani, and Pradeep Kumar Arya

6.1 Introduction

Today, Internet of Things (IoT) is being deployed to solve most of the present-day issues across many domains such as logistics, transportation, pollution monitoring, health care, home automation, smart city, smart office, infrastructure management, agriculture, energy (oil and gas) management, mining, and water efficiency. With the advent of wireless sensor networks, embedded systems, sensors, actuators, cloud services, micro-electromechanical systems, IoT has become very popular. It has ushered an era where smart objects are communicating with other smart objects, also called as machine-to-machine communication. These smart objects are capable to sense the neighboring environment, transmit and process the acquired data, and then give the response to the environment. Further, it is estimated that approximately a multi-billion of such objects would be connected by the year 2022, thereby impacting almost every sphere of our existence.

As a subset of IoT, Industrial Internet of Things (IIoT) presents huge opportunities for industrial transformation, viz. smart manufacturing processes, intelligent systems, sustainable production, automation, efficient asset management, stringent industrial controls, better supplier and customer relations, superior supply chain management, improved business outcomes, healthier ROI models, and operational efficiency along

S. Gupta
Department of Cybernetics, School of Computer Science and Engineering, University of Petroleum and Energy Studies, Dehradun, India
e-mail: s.gupta@ddn.upes.ac.in

G. Gabrani
Department of Computer Science and Engineering, BML Munjal University, Gurgaon, India
e-mail: goldie.gabrani@bmu.edu.in

P. K. Arya (✉)
Department of Computer Science, BML Munjal University, Gurgaon, India
e-mail: pradeep.arya@bmu.edu.in

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_6

with cost optimization. As IIoT mainly involves machine-to-machine communication, one of its major advantages is in automating the industrial applications without human intervention. However, both IoT and its subset IIoT also encounter many challenges while its actual realization takes place. In particular, the challenges are associated with the availability, reliability, energy efficiency, security, and privacy, resources with both limited power and computing capabilities, and so on.

6.2 What the IoT Is Made Up Of

An IoT environment consists of Internet-enabled smart things usually consist of sensors, embedded controllers, communication components, cloud storage, to collect, transmit, and analyze data they acquire from their environments. The collected data is sent to the cloud via IoT gateway for analysis. In some cases, the data may be analyzed locally. This complete process normally takes place without any human involvement. However, people may communicate with the objects to configure them, monitor them, issue commands, etc. IoT is extensively used for the applications and use cases covering domain of smart home, smart energy, smart health care, smart mobility, smart society, smart agriculture, smart building, smart government, and smart industry.

An important subset of IoT is the usage of the IoT in the manufacturing industry referred to as IIoT (Industry 4.0 or Industrial Internet). It needs special mention here as the manufacturing units form the basis of growth of any country. In other words, IIoT stretched IoT to include industrial domain as it is one of the most important sector far higher than domestic. IIoT initially meant an industrial framework where a good number of objects, devices, and machines can be connected to each other via communication technologies and software tools. Today, it is largely used in the space of IoT applications much beyond the consumer domain. It has many applications across a number of segments in industry in order to differentiate it from consumer IoT applications. It must be mentioned that the industrial domain is entirely different from the consumer domain as it requires specific communication protocols, stringent security requirements, Quality of Service parameters, etc. IIoT applications usually include sensor and actuator networks, cloud, web, industrial automation, robotics, embedded devices, and wireless sensor networks. Industrial Internet Consortium 2017 defined IIoT as ‘machines, computers, objects, and people enabling smart industrial strategies and processes using enhanced data analytics for transformational enterprise/business outcomes’. Systems of this kind are able to respond smartly and can manipulate their action depending on the data received via the feedback. This is in the perspective of Industrial revolution 4.0. It may be noted that all IoT use cases in Industrial revolution 4.0 are forms of IIoT but reverse is not true that is not all IIoT applications are about the industries which fall under the umbrella of Industrial revolution.

As mentioned above, IoT is transforming all the segments by acquiring much higher quantities of data, at much elevated rates, and much more efficiently. IoT is data-driven where huge amounts of data are collected, processed, analyzed, and shared in a manner that enhances the automation levels. The processed data provides valuable insights into the organization like never before. A number of pioneering organizations are implementing IoT by leveraging smart and connected devices in their units. In the same manner, data also has a vital role and is at the core of IoT. Implementation of IoT does not completely replace humans but greatly reduces their intervention by enhancing machine-to-machine communication. IoT focuses at optimizing and improving various industry processes in order to attain higher levels of automation. Even though this results in reduction of some specific types of tasks, this concurrently also generates the need of novel skill sets. As mentioned above, IoT adoption has nowadays become an essential enabler for the success of any organization, but it is also creating new security challenges for data, devices, and network. Traditional network security techniques and legacy processes are merely not prepared to tackle the rise of new IoT security issues. Today, IoT devices consist of more than 30% of all network-connected end points. It is the ripe time for security advisors to move past legacy solutions and create a complete creating an IoT security posture that allows IoT and protects the network from current and unknown potential threats. One of the most important solutions is the use of Intrusion Detection System as a critical solution to IoT security.

6.3 Intrusion Detection System

In the year 1980, Anderson conceived the notion of intrusion detection (Anderson 1980), and the application of this concept was done by Heberlein (1990). Heberlein developed a system and deployed it in a network to secure the network and referred to this system as Intrusion Detection System (IDS). An IDS continuously analyzes all the activities taking place in a network and hosts to prevent any sort of unauthorized access and also to detect any attack or malicious activity in the network. IDS, in general, includes both software and hardware to enable them to detecting cyber-attacks and generating instantaneous alerts. As an example, IDS may be considered as a software application that has sensors, an analyzer, and a reporting system that gives reports to administrator. Sensors are placed at different points of network or hosts. The sensors collect data and give it to the analyzer. The analyzer inspects the data to detect any suspicious or malicious activity. If an intrusion is detected by analysis engine, an alert is sent to the administrator of the reporting system to investigate (Rose et al. 2015). IDS hence behaves like a safety net to the network and the system consisting of hosts. IDS can be classified into four broad categories:

1. Host-based IDS
2. Network-based IDS
3. Protocol-based IDS
4. Application-based IDS

Host-based IDS are used for protecting hosts connected to the networks. These systems monitor the incoming and outgoing packets from the hosts and send the alert to the administrator in case of presence of any abnormal or malicious activity. These systems also scan the log and audit records in order to enforce security. This system is comparatively simpler than other types of IDS and has merits to analyze and give out detailed information and has much lesser false alarm rates. These types of systems are normally used in hosts being used mission critical applications, where changing the layout is a rarity.

Network-based IDS are used to detect the suspicious behavior in the network in order to find out the potential intrusions. These systems examine the entire traffic flow from all the devices connected on the network. It analyzes the traffic flow to investigate whether some known attack has taken place. At any moment, an attack is found or some suspicious activity is observed, the alert is immediately sent to the administrator of the reporting system. It is also sometimes installed on the network with firewalls to keep a check whether someone is attempting to break the firewall. The advantage of these systems is that they do not modify the host configuration, and hence, the operations of the business are not impacted. However, such systems only monitor the segment of the network connected to them directly without considering other network segments. Hence, to have encrypted sessions with these systems becomes quite cumbersome (Adat and Gupta 2018).

Protocol-based IDS is situated at the server's front end, and it analyzes the protocol information between the object and the server. It regularly monitors the https protocol to ensure the security of the web server.

Application Protocol-based IDS are generally configured at multiple servers. It finds out malicious activities by examining and interpreting the communication behavior on the protocols that are application specific. As an illustration, the SQL protocol could be monitored and it is used with the databases installed at the web server.

6.4 What Is Industrial Revolution 4.0, 3.0, 2.0, and 1.0?

Fourth industrial revolution is widely referred to as Industry 4.0. As per World Economic Forum, Cyber Physical Systems is the basis of the fourth industrial revolution. It involves amalgamation of the abilities of both human and machine. This is the period of IoT, AI, 3D printing, renewable energy sources, and self-directed vehicles. The third industrial revolution (3.0) instead was about digital technology and computers. Transistors, microprocessors, and Internet made processing and sharing information much easier and faster. Invention of electricity gave rise to the second industrial revolution (2.0). This led to the development of the automobiles, consumer products, and goods. During this time, the petroleum was found and steel was developed and hence their applications. The first industrial revolution (1.0) was related to water, steam, and coal. This era saw the development of steam engine and textiles.

6.5 Layered Architecture of IoT

Several multilayer IoT architectures have been proposed in the literature keeping into account the need to connect many heterogeneous devices among themselves and also to other digital platforms via bigger networks. Different layers help to divide a bigger IoT problem into subproblems, where each subproblem can be assigned to different layer. Each layer has specific functions, provides with different technologies, and has defined interfaces for providing interoperability. These architectures offer different services at each layer depending on organizational needs and technical requirements. Various popular architectures of IoT are given in Table 6.1.

It is easily observed from Table 6.1 that IoT architecture is entirely different from the 7-layered OSI architecture or 5-layered TCP/IP architecture as these architectures

Table 6.1 Various layered IoT architectures

Proposer of architecture	No. of layers	Name of layers
IoT WF (The IoT World Forum)	Seven	Physical, connectivity, computing on edge, data accumulation, abstraction of data, application, collaboration, and processes
ITU	Five	Sensing, accessing, networking, middleware, and application
Liu, Yang, and Liu	Four	Physical, transport, middleware, application
Domingo and Atzori	Three	Perception (sensing), network, service (application)
Xu, He, Li	Four	Sensing, networking, service, and interface
Flatt, Schriegel, et al.	3D architecture axis-six layers Process axis-value stream process Hierarchy axis-hierarchy levels	Six layers of architecture axis: Asset layer Integration layer Communication layer Information layer Functional layer Business layer
Purdue model for control hierarchy	Five	Physical processes, intelligent devices, control systems, manufacturing operations, business logistics systems
International Electrotech Commission	Three	Edge, platform, enterprise
Simplified IIoT architecture	Three	Things (sensors and actuators), communication network, applications

are not equipped to handle heterogeneous and distributed nature of sensors, actuators, machines, and other smart devices of IoT systems. IoT systems require efficient, real-time, and ubiquitous data aggregation protocols along with availability, flexibility, and scalability. IoT architectures vary from three layers to seven layers. The 7-layered architecture given by IoT WF is very straightforward and includes the data and control flow from edge devices (also called fog devices) consisting of sensors, actuators, machines, intelligent end-nodes, and other devices to the data analytics center or a cloud service. This architecture encompasses all networking components required for IoT connectivity, data reduction, data preprocessing, data filtering, data aggregation, conversion of data to information for proper storage and analysis by upper layers. The three-layer architecture International Electrotech Commission, instead, is a simplified model, in which edge layer devices connect with each other via LAN and to an IoT gateway. The IoT gateway then connects to the platform layer via bigger networks, thereby allowing much higher coverage. Finally, the platform layer makes connections with the enterprise layer which provides the domain specific applications and user interfaces.

It can be seen from Table 6.1 that nearly every architecture includes three basic layers, viz. things, communication network, and application. All these three layers consist of vast number of technologies keeping in view the heterogeneity of IoT devices and the different techniques that are available to connect them to a network. The communication network also incorporates a number of technologies as this layer offers both gateway and backbone technologies enabling the data to flow to central data center or cloud for further storage and analysis.

Now, briefly we will explain the three-layered architecture of IoT as shown in Fig. 6.1.

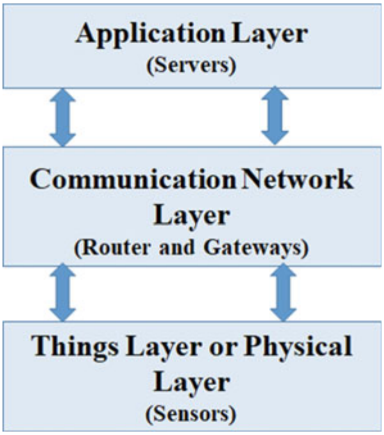


Fig. 6.1 Three-layered architecture of IoT

6.6 Layer 1: Things Layer or Physical Layer

Sensors, actuators, machines, and smart objects all are parts of this layer. This layer called things or physical layer is used to sense physical parameters from the environment. This layer deploys sensors for sensing and collecting data and information. This layer also recognizes other smart objects in the environment (Belkhiri et al. 2019). There are variety of ways in which things can be classified such as whether the object is (i) battery-powered or power-connected, (ii) fixed or mobile, (iii) low or high reporting frequency, (iv) low or high reporting range, (v) connected to other objects over a given area, and (vi) high or small form factor. The manufacturing units may have objects having different characteristics matching different requirements, thereby requiring a variety of IoT protocols and architectures. For example, if vibration of a certain machine exceeds a certain threshold, it may lead machine useless and unsafe. If the vibration sensor installed on the machine works on power, then it will have limited mobility, and if the sensor is battery powered, then it will have limited transmission range. Hence, before connecting these sensors on the network, such factors need due consideration. As this layer enables the physical things to sense, analyze, communicate, and perform some desired actions, this layer facilitates multiple applications, such as smart home, smart city, smart health, smart logistics, and so on.

6.7 Layer 2: Communications Network Layer

The main responsibility of the communications network layer is to connect to other smart objects, network appliances, edge devices, and servers. It is also responsible for reliable transmission and further processing of sensor data (Zegzhda and Kort 2007). Once the type of objects that are to be connected is decided (depending on various factors), next step is to connect these objects so that they can communicate. The design of communication network layer depends on many environmental factors such as temperature variances, humidity fluctuations, pressure variations, vibration measurements, gaseous nature, and type of power supplies. This layer can be further subdivided into four sublayers: (i) Access Network Sublayer, (ii) Gateways and Backhaul Sublayer, (iii) Network Transport Sublayer, and (iv) Network Management Sublayer.

(i) **Access Network Sublayer**
The type of access technology chosen varies for different IIoT applications and use cases. The choice depends upon the application requirements that is, which type of devices are being connected, what topology, how are they being connected, what type of data is being transmitted, at how much interval of time, and over what distance. Various technologies based on the range between the sensing device and information collector device are available, e.g., Bluetooth, ZigBee, IEEE 802.15.1, 6LoWPAN, IEEE 802.15.4, Wireless HART, Mi-Wi,

Near Field Communication (NFC), Bluetooth Low Energy (BLE) etc.; these are the guidelines specified by networking organizations both at national and international level like IEEE (Institute of Electrical and Electronic Engineers) or exclusive vendors that may be proprietary (Z-Wave by Sigma designs). These standards give the specifications of parameters like operating frequency, bandwidth usage, and power consumption.

(ii) **Gateways and Backhaul Sublayer**
Data collected from sensors through some access technology is first passed on to the gateway. Communication between the sensors and the gateway can take place through wireless or wired technologies. Sensors may be mobile or fixed, whereas gateway is generally static. The data collected on the gateway is forwarded to a cloud or some central server using another communication medium, usually wired, called the back haul network. Some of the technologies are Ethernet, Wi-Fi (2.4/5 GHz), IEEE 802.11ah (Wi-Fi bands 1 GHz), IEEE 802.16 (WiMax), and 2G/3G/4G Cellular.

(iii) **Network Transport Sublayer**
As discussed above, the communication in IIoT may be point-to-point or point-to-multipoint and occurs over multiple links of different types. It may be a short range wireless technology Wi-Fi or ZigBee inside a manufacturing floor or a longer range wireless technology WiMax to the gateway and another wired or wireless medium for backhaul transmission. Moreover, IIoT requires that communication protocols must be able to (i) support efficient and timely data aggregation, (ii) handle flexibility and scalability needs of sensors, and (iii) ensure availability (provide information whenever required). In order to enable such communication capabilities, a network protocol with specific properties is needed. IP and its different flavors, viz. IPv4, IPv6, RPL, and 6LowPAN, is a network protocol that meets all the above requirements.

(iv) **Network Management Sublayer**
Upper layer protocols are needed for data transmission between smart sensors and other applications. Multiple protocols have been defined for this by IEEE and ETSI (European Telecommunications Standards Institute). These protocols can be based on push or pull models. In push model, sensors send the data on regular basis on their own, whereas in pull model, the application asks sensors for the data. Hybrid approaches can also be used. Some of the protocols used are HTTP, MQTT, CoAP, XMPP, and AMQP. HTTP (Hypertext Transfer Protocol) is a very popular and widely used protocol based on client server model, where sensors are clients and the server is central data center. It is used for IIoT objects when they need to publish a lot of data. HTTP uses IP header for routing of datagram's. The data is not encrypted before transmission. HTTP, however, is a fat protocol and was not designed to use in the environments that have low bandwidth, low memory, and low power. In contrast to HTTP, MQTT—Message Queue Telemetry Transport—is a lightweight protocol especially devised for resource constrained devices used in IIoT applications. It has publish/subscribe architecture, where objects can publish and also subscribe for any topic and the data transmission takes

place after encryption. It connects objects and networks with applications using its three main components: (i) subscriber, (ii) publisher, and (iii) broker. The publisher builds the data and transmits the data to subscribers; this process is done via broker. The broker guarantees security by verifying the authenticity of both publishers and subscribers. It runs over TCP and allows one to many communication. CoAP (Constrained Application Protocol) was developed by IETF CoRE (Constrained RESTful Environments) for constrained devices. It is a lightweight protocol that runs over UDP, not TCP, and supports one communication. It employs DTLS to ensure secure data transmission. It uses a client server model in which client makes request to server and server send back replies. CoAP deploys RESTful architecture, that is quite similar to the HTTP protocol and also uses methods similar to HTTP (get, post, put, delete). XMPP (Extensible Messaging and Presence Protocol) is built on instant messaging and presence that enables data transmission between two or more systems. It supports many different communication patterns, viz. (i) request–reply, (ii) asynchronous messaging, (iii) event subscription (observe), (iv) publish–subscribe, (v) delayed delivery, and (vi) different QoS levels for messaging. AMQP (Advanced Message Queuing Protocol) is an open-source process that allows full functional interoperability for communicating messages between applications. Main properties of AMQP are (i) fast and reliable message transmissions and receipt of respective acknowledgments, (ii) distribution of messages in multiple-client environment, (iii) delegation of time intense tasks, (iv) enabling a server handle immediate requests quicker, (v) globally share and monitor updates between different connected systems, (vi) full asynchronous functionality, and (vii) improved uptime with respect to deployment of applications.

6.8 Layer 3: Applications Layer

The job of the application layer is to provide application-specific services to the users. It takes care of various applications in which the Internet of Things can be deployed efficiently, for example, smart homes, smart cities, and smart health. This layer of IoT systems is very different from application layer of an IT system. This is because IoT not only involves analytics of the data collected from the things layer but also provides for industry-specific control processes. The analytics applications layer gathers data from multiple things and smart objects, processes the data, analyzes it, and displays the result. The displayed result is intelligent enough to give insights into the data which otherwise would not have been possible.

The control applications layer instead controls the parameters of smart objects say a CNC machine or a lathe machine in a plant. An example is SCADA (Supervisory Control and Data Acquisition) systems that are used by manufacturing units to control and monitor industrial processes locally or remotely by collecting and processing real-time data. These applications interact with smart objects like sensors, pumps, motors, valves, and relays, thereby improving efficiency, enabling smarter decisions, and handling system issues to help lessen downtime.

6.9 Current Security Threats and Challenges in IoT

IoT is for sure creating wonderful experiences for users, but they provide new opportunities to hackers. These security breach activities are mostly hidden to the naked eye, and they are around us every time. Most of the IoT applications are ubiquitous and seamless (Chakravarthi and Veluru 2014; Saxena et al. 2017) and use multiple sensors, sophisticated microcontrollers, advanced software applications, and recent communication protocols for various applications such as smart homes, smart office environments, smart cities, and smart health; the outcomes are often amazing. Main gate of your house opens up when your car reaches near your home, the lights switch off when you leave the room; an equipment in the factory proactively goes into maintenance phase when some of its part starts malfunctioning. All these fascinating events also attract hackers who can inject malicious codes into your databases, attack websites, steal passwords, and make your systems redundant, and moreover, all these activities do not require their physical presence. So the organizations while taking advantages of the technological boom in IoT must also pay significant attention to the related security issues that come along with.

Even though IoT has many benefits, it has many challenges also such as energy efficiency, interoperability, security, and privacy of data. Out of these, probably security and interoperability pose the two major challenges. Interoperability between smart objects becomes an important issue as these objects operate in various industrial and manufacturing settings, have different architectures, and deploy different protocols. Moreover, as these protocols and architectures are not standardized, ensuring interoperability becomes difficult task. Each organization wants their data to be secure (Shreenivas et al. 2017; Lee et al. 2014; Mashal et al. 2015; Al-Fuqaha et al. 2015). The explosion of sensors and other smart objects that are communicated to each other via not so secure and properly encrypted network have given rise to security vulnerabilities (Saxena et al. 2017).

Some of the IoT security threats that must be taken care of are shown in Fig. 6.2 and described below.

1. Botnet

A botnet is a collection of various systems that together take control over a target's system remotely and distribute malware. The IoT and other devices which are connected via Internet then get infected by malware and permit hackers to readily control their operations. The botnet attacks include leakage of credentials, data theft, and access by unauthorized personnel and DoS attacks.

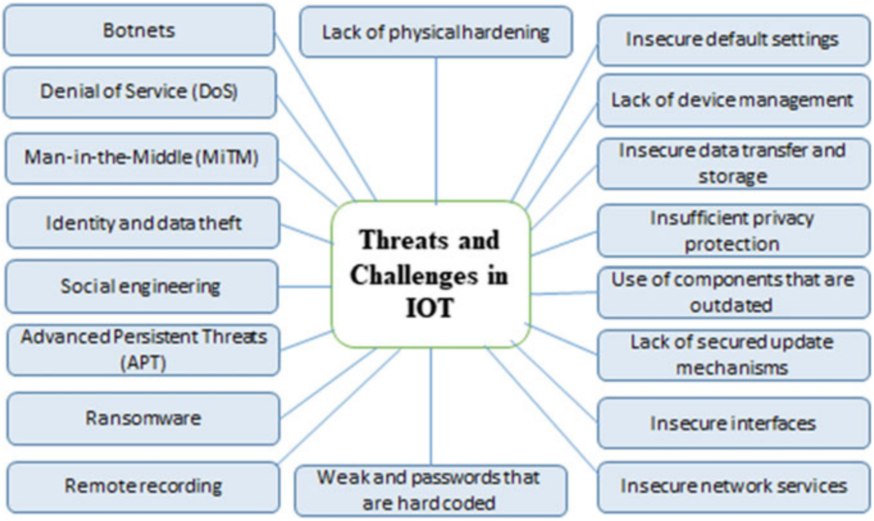

Botnets
Lack of physicalhardening
Insecure default settings
Denial of Service (DoS)
Lack of device management
Man-in-the-Middle (MiTM)
Insecure data transfer and storage
Identity and data theft
Threats and Challenges in IOT
Insufficient privacy protection
Social engineering
Use of components that are outdated
Advanced Persistent Threats (APT)
Lack of secured update mechanisms
Ransomware
Insecure interfaces
Remote recording
Weak and passwords that are hard coded
Insecure network services

Fig. 6.2 Security threats and challenges in IoT

2. Denial of Service (DoS)

When a hacker deliberately sends multiple requests to the target and creates a false capacity, a denial-of-service attack is said to have taken place. In this, the target server becomes unavailable by overwhelming input traffic from multiple sources. This is in contrast with phishing and brute-force attacks in which aim is to steal data, as DoS attacks are mainly used to partly or completely block a service and to damage the status of an organization and in turn impact their business. For example, a hotel which is facing denial-of-service attack will not be able to process requests for reserving new rooms, conference halls, wedding suites, checking room availability, etc. In this situation, the users may book other hotel for their services.

3. Man-in-the-Middle (MiTM)

In this attack, a hacker breaches and enters the communication channel between two parties. Hacker then intercepts the messages exchanged between them. First, the hackers get full control over their communication and then send illicit messages to both the parties. Such attacks are often used to hack IoT objects.

4. Identity and data theft

Recently, there have been multiple incidents of data breaches compromising the data of thousands of people. Secret information such as credit card details, telephone numbers, and email addresses were stolen and sold or misused. IoT devices such as smart refrigerators, smart meters, smart logistics, and smart home devices are also attacked by hackers to gain information about organizations.

5. Social engineering

Nowadays, social engineering is being used extensively by hackers to influence people so that they themselves reveal their confidential information. Hackers also sometimes for install malicious software into the target's system without his knowledge. These kinds of attacks normally involve phishing emails, to manipulate people to fall in their trap. These kind of attacks are much simpler to execute in case of IoT devices, especially on wearable technology. These IoT devices collect huge amount of information that is very personal to the user such as amount of money being spent, bank details, purchase pattern, and home address. With this information, hackers plan further attacks on user's connections through vulnerable IoT networks.

6. Advanced Persistent Threats (APT)

In this type of attack, a hacker wrongfully gets access to a network and then remains in the network without being detected for a considerable period of time. They regularly monitor network activity and steal critical data. Prevention and detection of these types of attacks are quite difficult Moreover, with the enhanced use of IoT devices, it has become possible to transfer huge volumes of data very easily. Hackers gain control of these IoT devices to confidential information (Pacheco and Hariri 2016).

7. Ransomware

One of the most notorious attacks is Ransomware attack, wherein malware is used to encrypt data that is essential for running operations of an organization. The attacker decrypts the encrypted data after he gets a ransom in lieu of this activity. It is one of the most important IoT security threats. For example, hacker can increase the temperature of air-conditioning plant and do not agree to bring it to the appropriate temperature until he receives the desired ransom.

8. Remote recording

Existence of zero-day exploits in IoT devices is a well-known fact to hackers to record conversations of people using IoT devices. As an example, video footages of day-to-day business activities can be recorded by using video cameras and then this information can be misused.

9. Weak and passwords that are hard coded

For hackers, it is very easy to break weak passwords by using a brute-force attack. This attack uses the entire list of possible passwords to find out the actual password.

10. Insecure network services

Insecure services running on the IoT devices connected to the Internet allows hackers to steal the critical data even remotely.

11. Insecure interfaces

This refers to the recent increase in the use of APIs, mobile apps, and web apps that allow users to transfer data with their smart devices. Any sort of vulnerability within these interfaces will lead to the compromising of IoT devices.

12. Lack of secured update mechanisms

One may unknowingly install malicious software from a hacker while updating his IoT device during the update process that is insecure. Hence, the updating has to be performed securely by using encryption technology and channels (Zhang et al. 2019).

13. Use of components that are outdated

By designing software's using outdated components, old operating systems, third party software from insecure suppliers leads to the security compromise of the IoT devices.

14. Insufficient privacy protection

Stealing of personal data from IoT devices can lead to privacy breach of users.

15. Insecure data transfer and storage

Each time data is transferred over a network, the probability of this data to get manipulated enhances. In order to avoid such contingencies, one must ensure that data is always encrypted before transmission.

16. Lack of device management

Proper management of IoT devices is extremely crucial or else the complete network could be hacked and all devices will be compromised.

17. Insecure default settings

IoT devices are often dispatched from the manufacturing units with not so strong default settings. Security attacks can take place if one forgets or is not allowed to change the default settings.

18. Lack of physical hardening

IoT devices are generally processed via hardening technology to safeguard them against physical attacks. Lack of hardening enables hackers to steal critical data either remotely or by taking full control of the IoT device.

In the literature, many intrusion detection schemes were proposed that aim to secure the communication over IoT networks consisting of sensor nodes, base station, cloud, and users.

Table 6.2 shows the computation cost, communication cost, and various challenges of intrusion detection techniques and cryptographic operations of related work.

This above analysis is very helpful to find out the consumption of power and energy in terms of cost by different schemes. This study gives a comprehensive view on how we may design an efficient intrusion detection techniques that provides better security measures with low computational and communication costs along with reduced overheads.

Table 6.2 Comparison of computational overhead, communication cost, and challenges in intrusion detection techniques

Intrusion detection techniques	Communication cost	Computational cost	Challenges of the schemes
Saxena et al. (2017)	6 messages	$3T_{\mathrm{EM}} + T_{\mathrm{I}} + T_{\mathrm{H}}$	False report injection, impersonation attack, denial of service, anonymity, gateway spoofing attack, forward secrecy, sensor spoofing attack
Huang (2009)	5 messages	$2T_{\mathrm{EM}} + 5T_{\mathrm{H}}$	Sybil attack, impersonation attack, password guessing attack, anonymity attack
Huang and Liu (2008)	4 messages	$5T_{\mathrm{H}}$	User anonymity, Sybil attack, password guessing attack, spoofing attack
Lee et al. (2012)	5 messages	$2T_{\mathrm{EM}} + 5T_{\mathrm{H}}$	Impersonation attack, password guessing attack, untraceability, spoofing attack

6.10 Conclusions

In this chapter, we have discussed the importance of intrusion detection system for IoT devices. We also discussed various types of IDS, their merits, and demerits. Different types of security challenges being faced by IoT devices and network were also discussed at length. In terms of further work, we believe that a lot of research and development is needed in the area of security and privacy of IoT devices. The increase in IoT devices and their applications in almost all areas of society also leads to the increase in different types of security breaches. Finding solutions to ever increasing variety of attacks also opens an area for future research. It has already started the fourth industrial revolution and is greatly affecting the industries today. It is projected that the industries today are proactively adopting IIoT technologies, and this inclination will continue and nearly fifty billion devices will be connected globally by 2020. Increased automation and with the use of flexible production methods have given around 30% increase in productivity. With predictive maintenance being deployed, around 12% is saved on planned repairs and maintenances, and breakdowns are reduced by approximately by 70%. In the future, technologists predict that IIoT will boost production quantities even more. Seeing these outcomes, industries are gearing up to create systems and processes to meet new requirements and keep pace with growing market speed. Organizations that have incorporated the IoT solutions along with appropriate security solutions bring about significant enhancements in connectivity, safety, privacy, scalability, efficiency, time savings, and profitability for themselves. In spite of all these benefits, IoT suffers from many challenges too, privacy, security, and constrained resources, naming, scalability, real-time performance, coexistence, interoperability, resource constraints, and mobility, being some of them. In view of all the above, we still feel IoT technology along with their security solutions are here to stay and impact our organizations working in various domains of health care, retail, manufacturing, logistics, etc., in a very positive way and bring about a paradigm shift in which our organizations work.

References

Adat V, Gupta B (2018) Security in internet of things: issues, challenges, taxonomy, and architecture. Model Anal Des Manag 67:423–441

Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor 17(4):2347–2376

Anderson JP (1980) Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, Fort Washington, PA

Belkhiri H, Messai A, Belaoued M, Haider F (2019) Security in the internet of things: recent challenges and solutions. In: International conference on electrical engineering and control applications, Constantine, pp 1133–1145

Chakravarthi SS, Veluru S (2014) A review on intrusion detection techniques and intrusion detection systems in MANETs. In: Proceedings of the international conference on computational intelligence and communication networks, Bhopal, 14–16 Nov 2014

Heberlein LT (1990) A network security monitor. In: Proceedings of the IEEE computer society symposium, research in security and privacy, Oakland, CA, pp 296–303

Huang HF (2009) A novel access control scheme for secure sensor networks. Comput Stand Interfaces 31(2):272–276. https://doi.org/10.1016/j.csi.2008.05.014

Huang H, Liu K (2008) A new dynamic access control in internet of things. In: IEEE Asia-Pacific services computing conference. https://doi.org/10.1109/APSCC.2008.116

Lee H, Shin K, Lee D (2012) PACPs: practical access control scheme for internet of things 2012. IEEE Trans Consum Electron 58(2):491–499

Lee T, Wen C, Chang L, Chiang H, Hsieh M (2014) A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN. In: Advanced technologies, embedded and multimedia for human-centric computing. Lecture notes in electrical engineering, vol 260. Springer, Netherlands, pp 1205–1213

Mashal I, Alsaryrah O, Chung T-Y, Yang C-Z, Kuo W-H, Agrawal DP (2015) Choices for interaction with things on Internet and underlying issues. Ad Hoc Netw 28:68–90

Pacheco J, Hariri S (2016) IoT security framework for smart cyber infrastructures. In: Proceedings of the IEEE 1st international workshops on foundations and applications of self* systems (FAS*W), Augsburg, 12–16 Sept 2016, pp 242–247

Rose K, Eldridge S, Chapin L (2015) The internet of things: an overview. Internet Soc (ISOC) 80:1–50

Saxena S, Sanyal G, Srivastava S et al (2017) Preventing from cross-VM side-channel attack using new replacement method. Wireless Pers Commun 97:4827–4854. https://doi.org/10.1007/s11277-017-4753-7

Shreenivas D, Raza S, Voigt T (2017) Intrusion detection in the RPL-connected 6LoWPAN networks. In: Proceedings of the 3rd ACM international workshop on IoT privacy, trust, and security, Abu Dhabi, 02 Apr 2017

Zegzhda P, Kort S (2007) Host-based intrusion detection system: model and design features. In: Proceedings of the international conference on mathematical methods, models, and architectures for computer network security, St. Petersburg, 13–15 Sept 2007, pp 340–345

Zhang D, Qiao Y, She L, Shen R, Ren J, Zhang Y (2019) Two time-scale resource management for green internet of things networks. IEEE Internet Tings J 6(1):545–556

Chapter 7
Malware Detection in IoT

Prachi Dahiya

7.1 Malware in IoT Software

Malware is an umbrella term used for all the malicious software that is used by the attackers to extract the information from a particular device. They can easily exploit the data of any programmable device that is associated with the Internet. This data can range from financial records, health information, personal emails and passwords, user login ids and their passwords, credit/debit cards data, etc. Hence, malware encompasses a lot of viruses, malicious software that are used by attackers in different ways in order to steal the information or with some revenge motives or assuming the control of the devices by giving the DoS commands back to back. Malware originated about 30 years ago, and since then, it has evolved itself to such a level that every device working today can easily be hacked or infected by malware. Some of the methods that are adopted by malware are malicious advertisements or malicious advertising, email attachments like phishing emails or just text messages, infected USB disk drives, and fake installations of software or some infected applications present on the system.

In simple terms, malware is malicious software which is used to gain access and damage a system or a device. IoT technology works fully on the Internet, and hence, it is more vulnerable to the malware attacks as they are always online and lack security. All the confidential information is present in the cloud online, and it becomes an easy way for hackers to access this information (Akhtar 2021). One must know that which malware attacks your devices suffer so that a detection algorithm can be used to locate the malware on the device. Other than this, one can easily identify if their device is infected by malware. There are some things that can be monitored like poor performance of the system, problems in shutting down your system or starting it, and browser always redirecting to a pirated site or to some pop

P. Dahiya (✉)
Delhi Technological University, New Delhi, India
e-mail: prachidahiya_2k20phdco11@dtu.ac.in

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_7

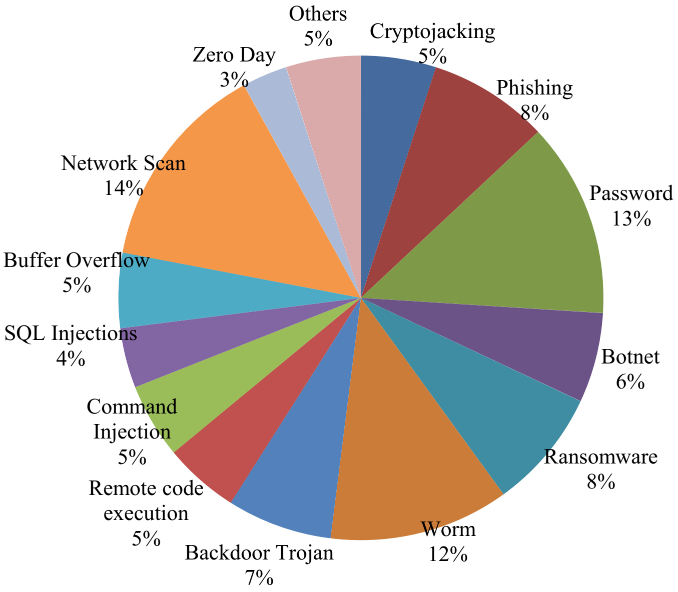


Fig. 7.1 Attacks by malware

ups. One can easily save their systems by limiting the number of applications on the device, never opening a pop up until and unless it is a trusted site, avoid clicking on links, fake emails from fake Web sites, etc. One can easily go for a security solution by installing some antivirus and perform regular security checks on the system such that no new malware is installed and you don't know about it.

A study was done in March 2020 is shown in the pie chart in Fig. 7.1 which shows the main reasons for the attack on the devices. The data were collected from June 2018 to 2019 of around 1.2 million IoT devices in various locations like health care and IT organizations. From and the results, we see that malware consists of 33% of the total attacks on the IoT devices which include botnet, Trojan horse, ransomware, and worms. Other than this, user practice is also a major contributor of 26%; this means that 26% of the attacks was done because of the negligence of the users with their security passwords and ids. 41% of the threats (Choo et al. 2020) and attacks was the exploits of the devices where the information of devices is present, and an attacker can attack it from a remote place through code executions, SQL injections, command injections, etc.

Malware is the most serious threat to the IoT devices. These malicious attacks work differently in IoT software and hardware. Most of the basic attacks work the software level. Figure 7.2 shows the different types of malware existing in the IoT software.

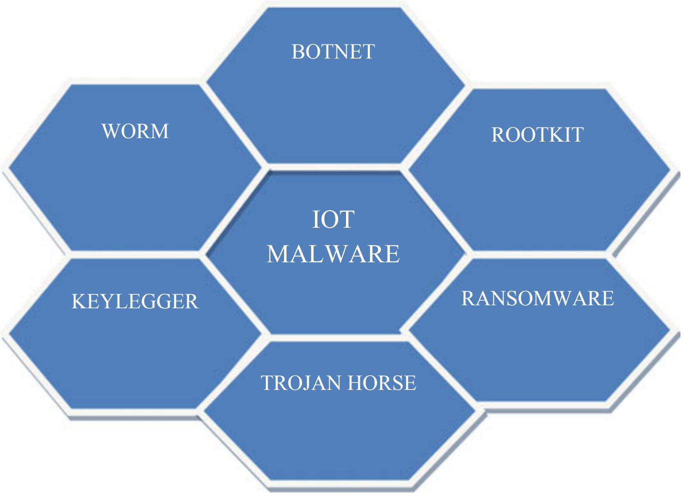


Fig. 7.2 IoT malware

7.1.1 Botnet

Botnet is a collection of several Internet-connected devices such as smart phones, computers, and several IoT devices whose security is breeched, and a third party can easily take the control of them. When a device is penetrated with software that is provided by a malicious software distribution and then the controller of the botnet is able to control all the bots or the affected devices. The architecture of the botnet has evolved and improved over the years in order to evade the detection and the disruption of the programs. Initially, bot programs are constructed as the client files which communicate with the other files over the server. The controller of the bots also called the bot herder performs all the operations from a remote location. Peer-to-peer network is used by the bots for communicating with each other.

Bots are self-propagating malware which target to infect the devices. They perform a distributed denial-of-service (DDoS), send spam to the infected device, steal the confidential data, etc. A large number of spams are sent to the target computer by the existing bots on the system such that the server gets overloaded and is not able to perform the basic functions in the system. They also provide access into the device to the attacker such that the attacker can control the device. All the bot-affected devices are subsequently connected with a server which is called "bot master" which acts as a central control hub for all the compromised devices. The bot master or the controller of the bots communicates with each other through a secure communication channel.

7.1.2 Ransomware

Ransomware is the kind of malware which threatens the victim to publish their data or block the victim out of their device until they pay a ransom amount to the attacker. Hence, the ransomware locks the user out of their device and asks for a monetary gain. Advanced ransomware uses crypto virology where cryptography is used to create malicious software. Here, it encrypts the user's device such that all the data of the device is inaccessible to the user. In a completely encrypted environment, a user must need to find a decryption key in order to get access to be data on the device. Finding a decryption key is also an intractable problem. Further, a screen locker ransomware is used to lock the screen of an Android TV, and a ransom is made for that.

Several ransomware software packages have come up in order to steal the user's money. Some of them are discussed. Riverton was a major ransomware Trojan in 2012 which made false accuses to the users like downloading illegal material and asked to pay the fine to the metro police department. Crypto-locker came in 2013 which worked by developing private keys for the users, and then, it threatened the users to delete the private key if they don't pay Bitcoin or online cash. WannaCry ransomware came in 2017 which affected around 2 million devices and demanded Bitcoin payments. Bad Rabbit is a Russian ransomware attack which encrypted the user's file tables and then asked for the Bitcoin payment to decrypt those files. In this way, ransomware has affected a lot of users and their devices and has put a lot of confidential information at risk.

7.1.3 Rootkit

Rootkit is a collection of malicious computer software designed to access unauthorized data. The term rootkit is a combination of two terms root and kit. Root is the traditional name for the Unix-based computer software, and kit represents the collection of software components present in the computer software that help in implementing a particular tool. The rootkit software can easily be installed by the attacker on the victim computer, and then, it can get easy access to the system's root or the administrator's access.

Rootkit is malicious computer software whose main aim is to access that area of the software which is otherwise not authorized. It often masks its existence in the form of software. Firstly, rootkit tries to gain the root or the administrator access. Obtaining the root access means a direct attack on the system which means exploiting the vulnerability of the system which is called privilege escalation. Privilege escalation means exploiting the design issues of the system or the system functionalities, etc. Once, the rootkit gets the direct access of the system then it can mask its intrusion from the user, and it can easily gain the important passwords of the system. Full control of the system also means that manipulations can easily be done in the system software.

Some detection methods for rootkit include the finding of a trusted operating system and some behavioral analysis.

Rootkit detection is done through behavioral-based approaches which mainly profile the system and look for any system irregularities and abnormalities such as differences in the time and frequencies, CPU utilization, and throughput. In signature-based approach, an antivirus is installed in the system, and it looks for the illegal signature detection or fingerprints, etc. Another approach is the difference based where the trusted and the tainted content is compared based on several levels, and then, difference analysis is done. Sometimes, rootkit detects the presence of the difference-based analyzer, and it adjusts it behavior which leads to no differences recorded.

7.1.4 Keylogger

Keylogger is also known as a keystroke logging, or keyboard capturing is a task to record the keys struck by the user on the keyboard without the knowledge of the user. The user is unaware that his actions are being monitored, and this data are recorded by the logger. Keylogging can also be done to study the keylog dynamics or to know the human interaction with the system. But, mostly, keyloggers are used to steal the confidential information of the users and the important passwords of the system. Keylogging exists for both software as well as hardware. There are several software keyloggers such as kernel based, API based, and JavaScript based. Hardware keyloggers include keyboard based, wireless keyboard and mouse sniffers, and firmware based.

When a keylogger is implemented at the root of the system such that it intercepts all the keystrokes that pass through the kernel, then that is keylogging at the kernel level. Hence, when keyloggers reside at the kernel level, then it becomes difficult for even user-based applications to detect that at which part the keyloggers are installed. In API-based keylogging, the keylogger registers itself on the application like a normal program. In JavaScript-based keylogging, the keylogger injects a malicious script tag targeted to the Web page, and then, it listens to all the major key events happening on that particular Web page. Hardware keyloggers consist of all the hardware keyboard components present along with the system. They include firmware-based key loggers, wired and wireless keyboards, keyboard overlays, acoustic keyloggers, electromagnetic emissions, optical surveillance, smart phone sensors, and body keyloggers.

7.1.5 Trojan Horse

Trojans are the malware which take over the system by stealing the user's identity and information. These are standalone malware, and they also help with the further attacks on the system by opening a backdoor. Social engineering is adopted by the Trojans which are the social manipulation of the people into doing something. They send a disguised email which doesn't appear to be suspicious; it is like a routine form, and the user is duped by this routine form or a fake advertisement. Trojans help the attacker to gain access to the information of the users their personal identity, their bank information, logging passwords, etc. Trojans can infect or delete or infect the user's files and folders connected to the Internet. Ransomware is also carried out by the Trojans.

Trojans do not inject themselves into a system like computer viruses, and worms; rather, they try to propagate through system's files and folders. After the installation of Trojans, they can perform a range of malicious actions, and they tend to contact the command and control (C2) servers across the whole Internet, and then, they wait for the further instructions. It is very easy to detect the Trojans in the system as they use only specific set of ports for the communication purposes. Hence, it becomes easy to detect them. Hence, Trojans can be a threat to the IoT devices, but they can also be easily detected because they have a very simple communication channel.

7.1.6 Worm

Worm is also a standalone malware which mainly replicates itself and can easily spread to different devices and computers. It mainly tries to enter a device when the security is down on that particular device, and it uses the computer network to spread. The infected computers or the worm-invaded computers are used as hosts by the worm to spread to the non-invaded computers. These behavioral methods continue till more and more computers are invaded (Damodaran et al. 2015). Recursive methods are used by the computer worms to exponentially grow and infect more and more computers in a short span of time. Worms cause very little harm to the devices, and many warms are designed just to pass through the computers and don't make any changes in the computer.

Most of the worms are designed not to be spread in the system, and hence, they do not attempt to change the system they are passing through. Worms don't need a host program to be setup rather; they work independently as a program, and hence, they are not restricted by the host programs and perform their attacks individually. They can take the advantage of several operating systems vulnerabilities in order to carry out active attacks. Some worms get combined with scripts and other technologies and can attack in different potential ways. They can easily access a Web page and can reside over there until they get triggered. Worms can not only infect local servers but can also affect a whole client server network based on a local computer. They can easily spread through different files and folders like Web pages, emails, excel sheets, and shared folders which contain large number of vulnerabilities in the network.

7.2 Malware in IoT Hardware

In the hardware, attackers have found different ways to attack the computer systems at the chip level which is very important part of the system. A minor modification at the chip level can lead to several different attacks, and the system can get compromised. The hardware of a system is formed by several strong algorithms and cryptographic functions. The attacker can easily manipulate with the cryptographic computations and can retrieve the authority. One of the most practical methods that can compromise the security of the device is the side-channel attacks.

7.2.1 Side-Channel Attacks

Side-channel attacks are cryptographic attacks which gain the information through implementing some computer algorithms, or rather, they try to find the weakness in one of the algorithms like cryptanalysis and software bugs. Side channels act as a black box attack when technical knowledge is used to know the internal functioning of the system. Power consumption of the system, some electromagnetic leaks from the system, can also provide the information to the attackers about the system hardware. This information coupled with some appropriate calculations can lead to the retrieval of the secret key by the attacker. Side-channel attacks are divided into two parts: active and passive.

Passive attacks mainly work toward the collection of information from various places in the system, and hence, the useful information is gathered during the operation process of the system. While the active attacks not only gather the information, but they also work in a dynamic format. Through an active attack, an attacker can easily retrieve the secret keys of the system by the injection of some faults in a normal function operation. Special equipment consisting of amplifiers, probes, analyzing software, etc., are used during the information gathering done through a side-channel process.

There are a lot of types of side-channel attacks that are discussed below:

(i) Cache Side-Channel Attacks: These attacks work by focusing on the security of the critical operations of a system such that they can get access to the confidential data of the system like passwords. The attacker can retrieve the secret key of the system which mainly depends on the accesses that are made by the victim system, and in this way, the attackers also gain the encryption key of the system. Cache side-channel attacks do not focus on finding the faults in the cryptographic operations happening in the system, and this is why, they are invisible to the victim system. Some of the CPU vulnerabilities are exposed to the attacker and which allow the cache-based side channels to leak the confidential information to the public as the memory of the system is exposed to the attacker.

(ii) Power Analysis Side-Channel Attacks: As the name suggests, this attack follows the energy consumption of the CPU of the system. It mainly looks into the power consumption of all the hardware devices attached to the system as well as it monitors the cryptographic circuits. Based on the energy consumption of the devices, these attacks categorize into simple power analysis (SPA) and the differential power analysis (DPA). The fluctuations in the current are measured and observed daily, and the radio waves generated by this current are also observed. Similar statistical techniques are called as power analysis attacks as a compound term given by the power analysis side-channel attacks.

(iii) Timing Side-Channel Attacks: This side-channel attacks observe the time taken by the data to go in and out of the CPU of the system. It also looks for the data movement on the hardware that is running the cryptosystem or the algorithm of the program running on the system. Simple variations are observed by these attacks that how long does it take to perform a particular cryptographic operation, and this may help to determine the complete secret key of the system. These attacks involve the statistical analysis of the timing observations and measurements and can be demonstrated across the networks for the systems to analyze them properly.

(iv) Acoustic Crypto-Analysis Attacks: This attack deals with the power consumption of the devices. Temperature changes can create a thermally induced stress which is mechanical stress, power consumption causes the devices to heat up which causes stress to the cooling stress. This stress at different places in the hardware of the system leads to the acoustic emissions. Recent researches show that by the knowledge about the operations of the cryptosystems and the related algorithms, the attackers can get a lot of confidential information about the system.

Other side-channel attacks include thermal imaging attacks that look into the infrared images which may provide the information about the code that is executed on the CPU. Optical side-channel attacks include the gleaning information which contains the hard disk activities and look for the small number of photons emitted by transistors as they change state. Another type of side-channel attacks includes allocation-based side channel attacks which are based on the information leaks that are from the allocation of a resource to the network.

7.2.1.1 Counter Measures

There are basically two main categories for the counter measures based on the relationship of the leaked and emitted information with the side channel:

(1) Elimination or the reduction in the release of the leaked information;

(2) Eliminate all the relationships existing between the leaked information and the confidential information which will make the leaked data unrelated with the

system from where it leaked. In a way, it becomes uncorrelated. The randomization of the ciphertext is done in such a way that it cannot be changed even after the cryptographic operations.

Special shielding methods are used in the first category in order to lessen the release of leaked information, to lessen the electromagnetic emissions, reduce the susceptibility to the attacks. These shielding tools and methods are available commercially today. Powerline filtering and conditioning is done in order to help in monitoring the power consumption attacks on the system. These measures should be taken cautiously as a slight relation of the leaked data with the system can be a threat to the security of the system (Ngo et al. 2014). Physical enclosures are used for stopping the installation of any hardware devices with the system like microphones and other micro-monitoring devices which can be used for any kind of leakage.

The channels can be jammed also which are having noise. This counter measure also comes under the first category; the analysts can jam the emitted channel easily with some noise. Random delays can be done for the emission of the channels in order to deter mining the impending attacks. For these delays and jamming of the signal, sometimes, the adversaries improve themselves and compensate for these delays by sending more than one signals over the channels and by averaging a lot of measurements for the analysis part. So, the collection of more measurements is done by calculating the delays in the signals.

The side-channel attacks can be categorized as they are found in the different design stages of the system hardware with underlying qualities and features. The security analysis software is used by the defense team to identify different classes of the side-channel attacks like cache attacks and timing attacks. Certain security analysis and software platform are available for testing the system for any vulnerabilities, and then, they look for any architectural changes in the system and if there is any security breech happening. Another method to develop a counter measure is to create a security development lifecycle of the hardware; it is deployed with all the security analysis platforms present in the system on several levels of the development lifecycle.

Timing attacks are done based on the computation time on tasks and operations performed in the system, and these computation times are recorded into discrete clock cycles in a quantized format. The only countermeasure to deal with the timing attacks is to form a software which is isochronous which makes a format that the operations will run on the system up to a particular amount of time independent of the secret values. This measure helps to eliminate the timing attacks against the system. These type pf countermeasures are hard to implement in today's world as every operation instructions have a varying timing on the CPUs.

Partial countermeasures are used against power attacks by designing software called as PC-secure, and it is used in the program counter security model. In the system, which contains a PC-secure program, there the execution does not depend on the individual secret values of the system. The architectures where the instruction execution time is data independent, there these PC-secure programs are immune to the timing attacks on the system (Tahir 2018). Another way is that the code should be non-isochronous as the PCs have a memory cache from where the data are accessed frequently by the users of the system, and hence, there is no particular time limit. This leads to the time penalty where the information about the usage of the memory blocks is leaked sometimes by the timing attacks. For such things, cryptographic code is designed and implemented to mainly resist the cache attacks when they attempt to use the memory as predicted by the countermeasures.

7.3 IoT Malware Analysis Techniques

Malware analysis is a major step toward the malware detection in the system. The analysis techniques mainly study and analyze the malware, how it is formed, how it is propagated into different systems, what are the major functions of a malware, etc. Hence, the purpose of these analysis techniques is to understand how a particular malware works, and what the purpose behind the development of a malware is (Tawalbeh 2020). The analysis techniques help the detection techniques in forming a defensive functionalities and algorithms against the acting malware. Some of the analysis techniques are described below.

7.3.1 Static Analysis

In static analysis, the executable files are examined without looking into the actual instructions. A basic static analysis firstly confirms that the file is malicious; then, it provides all the information about the functionality of the malware, and in the end, they will allow you to produce some simple network signatures. Static analysis is a quick process and is quite a straightforward process. It is a simple and easy process that is why it is mostly ineffective against a strong malware, and it can also miss some of the important behaviors of malware. Static analysis can be done through different approaches, and some of them are discussed below.

7.3.1.1 Searching Through Strings

The strings are the easiest way to know the functionality of a program. Any file contained in a system uses some hard-coded data mainly contains some URL's, messages, file paths, addresses, etc., and these all contain strings inside them. Hence, these strings can provide a great deal of information about the attacking malware. Whenever a program accesses a URL or an IP, it may indicate that the malware is going to attack through some network functionality of the system. When the strings search for an executable for ASCII or UNICODE, then the formatting and context are ignored, and one can easily analyze any file, and the strings can be detected across an entire file format. Examples of strings through which some important information can be collected are given as: cmd: Strings <filename> files can be searched through this command using the utility strings.

Besides using string, some important information can be collected statically from the malware is through loaded libraries and some imported functions. The functionality of the malware can easily be guessed from these libraries and functions. For example, if the malware uses "kernal64.dll", then they import the function "Create Process Z" indicates that a file will create a process called Z at the time of the execution. If the malware uses "ws2_64.dll" means that the malware is going attack at some of the network functionality of the system.

7.3.1.2 PE File Format

A portable executable (PE) file format is also used by the windows executables, objects codes, and direct link libraries (DLL) which contain the code that can be used at more than one place. PE file format acts as a file data structure mainly contains the wrapped up executable code which is manages by the operating system loader as it contains important information. Almost, every file contains the executable code which is present in the PE file format. This is why malware mainly targets the PE files because they contain the important information about the system code and DLLs.

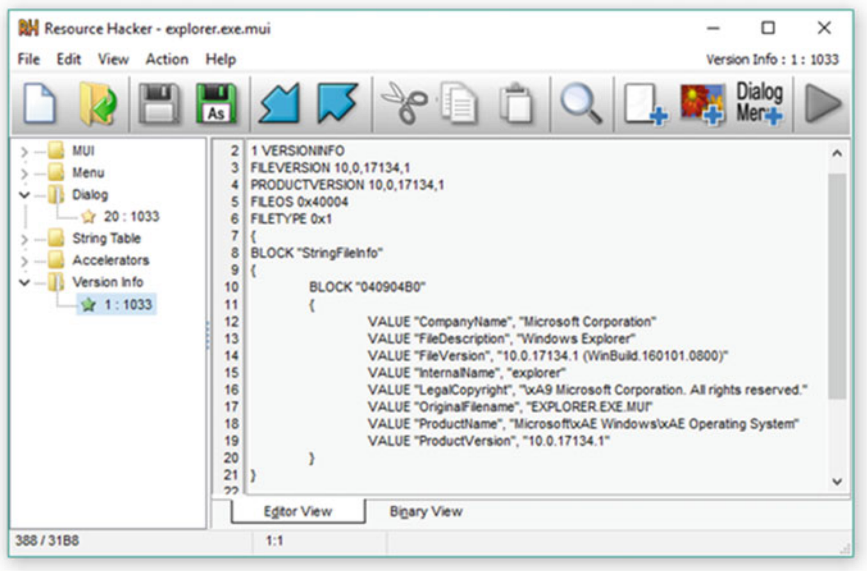
7.3.1.3 Dig for Resources

As mentioned in the previous section that the PE file format contains several headers as well as the sections. Other than these file formats, one can look into the resource section which is given by the extension called .rsrc. This resource section contains several things like icons, images, videos, and various language strings are stored. Due to the contents of this resource sections, the malware authors try to hide their executables in this section that will be used by malware directly at the time of execution in the main program.

Resource hacker is a free-resource extraction compiler for the windows developed by Angus Johnson. This utility-based resource is used to ass, replace, or modify the resources in the windows including its strings, images, menus, and dialog boxes. Hence, to look for the suspicious or the malicious strings or resources inside the programs, one can use this resource hacker application easily. Figure 7.3 shows a window for searching of malware component inside a company file.

7.3.2 Dynamic Analysis

Dynamic analysis mainly executes the code in a safe environment where it suspects that a malicious component exists, and this whole process is termed as a sandbox. When the code runs, the security professions a look for the suspicious malware



```
1 VERSIONINFO
FILEVERSION 10,0,17134,1
PRODUCTVERSION 10,0,17134,1
FILEOS 0x40004
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
        BLOCK "040904B0"
        {
                VALUE "CompanyName", "Microsoft Corporation"
                VALUE "FileDescription", "Windows Explorer"
                VALUE "FileVersion", "10.0.17134.1 (WinBuild.160101.0800)"
                VALUE "InternalName", "explorer"
                VALUE "LegalCopyright", "\xA9 Microsoft Corporation. All rights reserved."
                VALUE "OriginalFilename", "EXPLORER.EXE.MUI"
                VALUE "ProductName", "Microsoft\xAE Windows\xAE Operating System"
                VALUE "ProductVersion", "10.0.17134.1"
        }
}
```

Fig. 7.3 Resource hacker

activities in action. As the code is running in a safe environment, the malware is not able to infect the system of the enterprise network. The dynamic analysis allows the threat hunters as well as the incident reporters of the malware with a very deep visibility into the malware functionality, and this can help them in knowing more about the true nature of the malware. Reverse engineering time can be saved through sandboxing which helps in discovering of the malicious code (Tewari and Gupta 2018). The main challenge that exists for the dynamic analysis is that the malware code has become more and more smarter, and hence, enhanced sandboxes are used today which have also become somewhat good at detecting the malware. Sometimes, malware is able to deceive the sandbox by hiding code inside of them, and hence, they remain dormant till all the necessary conditions are met.

Dynamic analysis executes the code first in order to analyze any malware and observe its actions existing in any of the code that is being run. There are various levels at which the analysis of malware can be done. The lowest level is the binary code that exists for the whole system where the changes can be made for the registry or the file system. The main purpose of the dynamic analysis is to expose the executable malware, while it is still running, and it should be done in such a way that malware does not compromise the security of the analysis systems on which it is running. There is a risk of malware infecting the system because when the dynamic analysis is done, the malware is then loaded into the memory of the system which means it is loaded into RAM, and then, it is executed by the host CPU.

Dynamic analysis looks for the meaningful patterns as well as the signatures that can easily tell the maliciousness of the analyzed file. No such thing happens in the static analysis which analyzes the binary code which can take a lot of time and that is why dynamic analysis doesn't rely on the binary code analysis. This is why the static analysis is vulnerable to a lot of evasion techniques such as obfuscation and packing. Other than this, the dynamic analysis does not translate the binary code into the assembly level code through a disassemble. This is so because the disassembling the binary code is a simple and straightforward process, and hence, the attackers can use different techniques to change the binary code, and there is a possibility that the binary code has been changes, and in actual, the malware is being loaded into the system and then executed. The dynamic process does not rely on the disassembling process, and it is immune to the several evasion techniques of the malware. Static analysis is not able to detect the changes that are made in the code during its execution, while dynamic analysis is immune to this effect.

7.3.2.1 Malware Sandbox

Dynamic analysis uses the malware sandbox in order to analyze the sophisticated and complicated malware attacks and find ways to strengthen their defense mechanisms. A deep analysis of malware is done and for the unknown threats and this helps in improvement in the sandbox system to mitigate some threat intelligence measures (Tiwary 2020). The key features of a malware sandbox include an in depth search into the file or folder which is thought to be affected by the malware. Intuitive reports are generated for the characteristic features of the malware and how to tackle it. Figure 7.4 shows different features of a malware sandbox. It uses user interactions as a medium to find out the user actions in the system. Environmental awareness is a prospect of sandbox to know the real-life events happening in the sandbox-related processes. Data obfuscation is done; some encryption API calls are used by the sandbox. A complete system analysis is done by the sandbox to know the characteristics of the malware if present in the system.

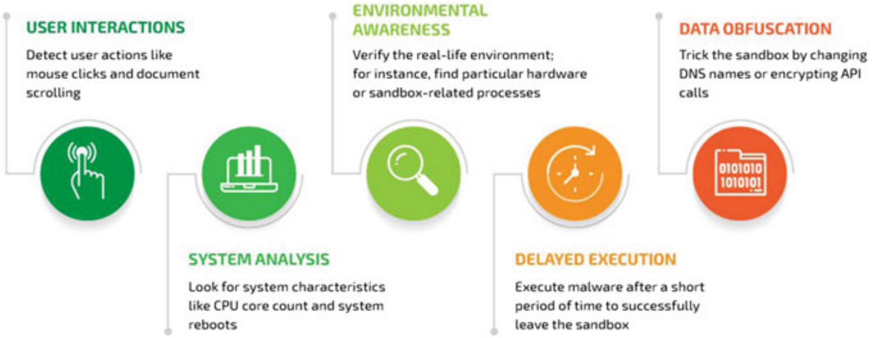

USER INTERACTIONS
Detect user actions like mouse clicks and document scrolling
ENVIRONMENTAL AWARENESS
Verify the real-life environment; for instance, find particular hardware or sandbox-related processes
DATA OBFUSCATION
Trick the sandbox by changing DNS names or encrypting API calls
0101010
1010101
SYSTEM ANALYSIS
Look for system characteristics like CPU core count and system reboots
DELAYED EXECUTION
Execute malware after a short period of time to successfully leave the sandbox

Fig. 7.4 Malware sandbox

Falcon Sandbox is one of the major malware detection sandbox that is been used today by various dynamic analysis techniques. The detection of unknown threats is done by this sandbox with zero exploits or any harm done to the system. All data are analyzed and automatically engineered into the malware reports. Sometimes, to tackle the sophisticated malware, sandbox is converted into the anti-evasion technology which includes a state-of-art detection mechanism which is not visible to the user mode applications. Similarly, to the user applications, these anti-detection technologies are not easily identified by the existing malware, and this sandbox remains undetected by the malware, and it can work toward detecting the malware and analyzing it. The sandbox can be customized according to the date/time, functional variables as well as user behavior is taken into consideration.

It is very important to find out insights about the malware that is being analyzed such that one can know what the main purpose behind the malware is and what are some unique qualities of the malware, and also, to determine, which are the file systems that are to be affected by the malware. It is also necessary to know that what type of malware it there and what family does it belong to. A Falcon Sandbox can search into the biggest malware search engine that is in the cybersecurity industry, and it finds out the related malware samples, and within seconds, the analysis is then expanded to all the system files and folders. This analysis is very important for getting a better insight and a deep understanding into how the attack is planned by the malware. It also helps in making a better protective system for the organization such that the no such malware can attack the system again.

In order to achieve full visibility of the malware, it is required to get an in depth insight into all the files, memory of the system activities. Reports are made in such a way that the analysts can easily read these reports and can be effective in their given roles. Practical guidance on how to deal with the threats, their prioritization, and response is given by the reports. These reports help IR teams and the threat hunting teams on how to proceed once the threat is detected and what necessary steps should be taken to get a deeper analysis of the malware. The Falcon Sandbox provides a wide range of executables, file formats, image formats, scripts, strings, and even some archive files that analyze around 40 different file types to know more about the malware. This is all supported by Windows, operating systems, Mac Books, Linux as well as the androids for the mobile computing.

7.3.3 Hybrid Analysis

Hybrid analysis is the mixture of static and dynamic analysis, and it supersedes both of them. The problems of both static and dynamic analysis are canceled out in hybrid analysis. Static analysis is not effective when the attack is done by a sophisticated malware, and at times, this sophisticated malware hides itself so well that the sandbox dynamic analysis is not able to detect it. Hence, by combining both the static and the dynamic analysis detection techniques, there is a way that hybrid analysis can provide with a security team for the system that will be the best of both

Table 7.1 Differences in the malware analysis

Static analysis	Dynamic analysis	Hybrid analysis
Static analysis does not run the code and then try to analyze the malware binary code	Dynamic analysis executes the code, and the code is looked closely to find the malicious code in the virtual environment	Hybrid analysis is used to detect the sophisticated malware which is not easily detected by static and dynamic analysis
Signature-based approach is a used here which is a detection technique for IoT malware	Behavioral-based techniques are used in the dynamic analysis	Hybrid analysis uses a mixture of signature-based and behavior-based approaches
This analysis uses file fingerprinting and signatures, debugging, code obfuscations, reverse engineering methods and several other detection methods	Dynamic analysis includes system calls, API calls, instruction sequences, network traces, memory writes, and several more methods	Hybrid analysis mainly detects the malicious code through the indicators of compromise (IoCs)
This analysis method is very much ineffective against the sophisticated malware and malware code	Execution is done in dynamic analysis, and hence, this method is effective against all the sophisticated malware	Hybrid analysis tries recognize the malware through static analysis, and further work is done by dynamic analysis

the approaches (Wazid 2019). Primarily, this approach will detect the malicious code which is trying to hide somewhere in the code through static analysis, and then, all the indicators of compromise (IoCs) are extracted statically from the previous unseen code present in the system. Hence, one can say that the hybrid analysis techniques can even detect the sophisticated malware which is detected neither by static analysis nor by dynamic analysis.

Behavioral changes are looked into such as when a piece of malicious code is being run and then it makes some changes in the memory. Hybrid analysis applies static analysis to look for the behavioral changes in the data. Hence, basic static analysis is applied on the memory dump as provided by the system. A dynamic analysis also detects the necessary changes and then alerts back the malware detector. In the end, IoCs are exposed, and hence, zero exploits are also seen. Table 7.1 discusses the major differences in different ends of analysis. They are given.

7.3.3.1 Stages of Malware Analysis

There are a certified number of stages in the process of malware analysis and detection techniques. Each and every static and dynamic property is being analyzed. Behavioral analysis, fully automated analysis, manual code reversal analysis techniques are undertaken by the experts. Some of the analysis methods are given below.

7.3.3.2 Static Properties Analysis

Static properties mainly include all the embedded strings present in the malware code, hashes, metadata, some header details, and some embedded resources. This data are mainly required to create the IOCs, and then, they can be acquired very gently and quickly as the requirement to run the program is over as the proof that the malware exists is with the system. Static analysis gathers the insights about the features and functionality of the malware such that one can decide whether a deeper investigation about the malware is required or not. Comprehensive techniques can be used by the analysis team to gather what necessary steps can be taken further in order to minimize the attacks of malware in the system.

7.3.3.3 Interactive Behavior Analysis

Behavior analysis of a malware can be determined by observations and reports as well as by interacting with a malware sample inside a lab. This may help the analysis team in gathering information about the behavior of the malware that how it reacts under certain conditions and what set of commands can trigger the malware to behave in a particular way. The analysts also get the knowledge about the files and folders which will be affected by the malware, their processes, activities, etc. Memory forensics is used by the analysts to analyze how the malware uses the memory of the system.

If some of the capabilities of the malware are observed by the analysts, then a simulation test is being used in order to mitigate the attacks caused by the malware in the system. For such advanced analysis and observations of the malware, the system requires a creative set of analysts who have very advanced skills in order to deal with these sophisticated malware. There is also a need of automated tools in order to analyze these complex and complicated malware. Hence, to get effective and better results, there is a need to get creative analysts and complex automated tools.

7.3.3.4 Fully Automated Analysis

Fully automated analysis mainly assesses the malicious files and folders in a simple format and very quickly. Possible repercussions are formed by the fully automated analysis for the malware which may try to infiltrate the network the system is using. Hence, this analysis provides an easy-to-read report which may provide very fast solutions and deep insights into the malware. The security teams can benefit largely from the automated analysis due to their fast and simple working. Hence, they are the best way to process a malware at a particular scale.

7.3.3.5 Manual Code Reversing

The code is reversed over here manually by the analysts by using some disassembles, debuggers, compilers, etc. Reverse engineering of a program or a code is the basic task that is completed by the manual code reversing. With the help of some specialized and automated tools, the analysts are able to decrypt the encrypted data, and hence, they put in an effort to find the logic behind the malware source code as well as its algorithm, and then, they are able to observe the hidden capabilities and features of the malware which it has not even exhibited till now. Code reversal is not an easy task, and hence, it takes a great deal of time to complete this task. Due to its time consumption issue, code reversal is skipped by a lot of malware analysts and investigators, and then, they miss out on a lot of insights that could have been gotten through code reversal. Although code reversal is a slow process, but it provides some powerful insights about the malware.

7.4 IoT Malware Detection Techniques

The increase in the malware in the IoT devices has led to the development of a number of protection and detection techniques. These methods not only detect the malware but also provide the affected system with some countermeasures to remove the malware from the system. Despite a large number of protection and detection methods, the IoT devices are still not safe from the malicious activities (Zhang 2014). There is a need for a stable and an efficient detection and protection method. Some of the popular methods are given below. Figure 7.5 shows the different detection techniques.

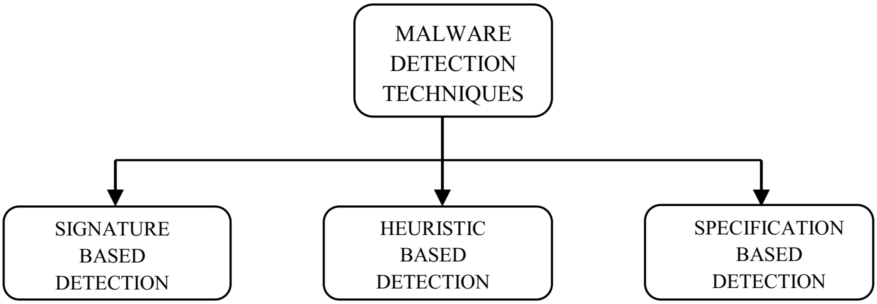

MALWARE DETECTION TECHNIQUES
SIGNATURE BASED DETECTION
HEURISTIC BASED DETECTION
SPECIFICATION BASED DETECTION

Fig. 7.5 Malware detection techniques

7.4.1 Signature Based

When a malware is embedded into a code, then a sequence bit is generated inside the code which is known as the signature bit which is used to mainly identify the family of the malware to which it belongs to. Most of the antivirus programs use the signature-based detection techniques to provide better strategies in order to secure the system. The code in which the malware is embedded is disassembled by the signature-based detection methods such that the pattern can be searched in the infected file, and the family of the malware can be known. A database is maintained which contains the details of the signatures of the malware, and they are used for the comparison purposes later on. These kinds of detection techniques are also known as pattern matching or scanning. There are three types of signature-based detection techniques which are static, dynamic, and hybrid detection.

Signature-based detection is mainly used in the cybersecurity systems and mainly follow and scan the footprints of the malware and identify them. These footprints in cybersecurity are called digital footprints that are left by all the programs, files and folders, software and hardware, applications, etc. These all footprints are unique in some way, and the antivirus software is able to detect the malware and can know which family the malware belongs to.

Hence, the main working of the of the signature-based detection techniques starts by searching the system if a malware exists by looking at the footprints of different programs that are running in the system. Next thing that happens is that the details of the footprints of the malware are stored in the database for the comparison. After the footprints are analyzed and observed to know which malware the footprint or the signature belongs to and then if a footprint is recognized and the malware is known, then the malware footprints are either deleted or isolated such that the malware cannot affect the system anymore.

Signature-based malware detection is one of the best methods to find out the malware residing on a system and is used by many antivirus software and products. Malware is a kind of malicious software which also leaves a footprint behind, and whenever this malware's footprints are discovered, then these footprints are added to the database. From this database, the malware is compared with others, and its family is detected from the database. Then, it becomes easy for the antivirus software to detect the same malware on different IoT devices.

Stepwise signature-based detection:

1. A new malware is found in the system.
2. The footprint of malware is added to the database.
3. Database is updated by adding new malware.
4. Scanning of malware in the system is done by antivirus software in the system.

7.4.2 Heuristic Based

The heuristic-based malware detection technique mainly finds differences between the normal and the abnormal behavior of the system such that one can find the known and the unknown attacks of the malware such that they can easily be identified and then resolved by the antivirus software present in the system. The heuristic-based detection technique works in two parts. Firstly, the normal behavior of the system is kept in check and observed when there is no impending attack on the system. The normal behavior of the system is being kept securely and then verified and checked such that one knows that how the system works when it gets attacked. Whenever the system is attacked, the differences in the normal and the abnormal behavior are checked and kept securely. In the second step of the process, the family of the malware is detected such that the features and functionalities of the malware can be known.

Heuristic method detects the virus in the system by examining a particular part of the code which is found suspicious or having some malicious motives for the system. Traditional methods which include signature-based detection method compares the code or the program in order to identify the malware with the virus and the malware that has already been encountered by the antivirus software, and hence, an analysis is done and recorded in the database. There are various disadvantages to the signature-based method as the threats and attacks have evolved themselves a lot, and hence, the signature method has become limited. These threats are coming up everywhere and are now immune to the signature-based method and are not detected easily these days. This is why heuristic-based detection technique is a better option.

Heuristic-based detection technique overcomes all the disadvantages of the signature-based technique as it is mainly designed to find the suspicious malware activities happening in the system. Heuristic-based technique spots the characteristics which are malicious activities found in the system; new viruses can easily be found and even their modified versions and the existing threats in the system. Heuristic analysis is sometimes used to deal with the cyber-criminals who constantly give threats to the system by exposing the confidential information. Heuristic analysis can easily deal with a large volume of threats that are made to the system on a daily basis. Heuristic methods are the only one that can deal with the polymorphic viruses which are mainly malicious code that keep on updating themselves and adapt to the environment of the system and hence, change constantly. Advanced security solutions are combined with the heuristic analysis such that they can find out the new threats as soon as possible before they can harm the system without the need of a specific signature.

Heuristic method contains different types of techniques under it. One of them is static heuristic analysis which includes the disassembling of the suspicious piece of code that probably contains malware, and this code is examined and observed that how it reacts under certain conditions. If a malware is detected in the code, then it is compared with the already existing malware and virus in the heuristic database of the system. If a particular part of the code matches the database, then that particular part of the code is flagged as a possible harmful threat. Dynamic heuristics analyze the suspicious code and then observe it and perform tests in a secure environment. This method mainly observes how the malicious code reacts and behaves in different critical conditions but in a secured way.

Sandbox is also used here as it is observed how the suspicious code works inside the specialized virtual machine. The sandbox system allows the antivirus software program to test the malicious code and simulate the results that what would happen if the malicious code acts or a suspicious file is allowed to run during its favorable conditions. Each and every action is examined of the acting malware that how it gets activated, what is favorable conditions, its functions and functionalities, its suspicious behaviors which may include spam, self-replication files, and several other actions that are very common for the viruses.

The main aim of the heuristic analysis is to identify the new threats that come up, and they have to be constantly improvised such that the best possible detection can be provided for recognizing new threats without generating the false positives on the valid code which doesn't contain any malware. Hence, due to this, the heuristic tools are combined into one sophisticated antivirus software. These heuristic-based methods are deployed with all the other malware detection methods such as specification-based techniques, signature-based techniques, and other proactive technologies.

Although there are several functionalities and features of heuristic-based detection techniques, but the limitation are always there for it needs a lot more of resources, and the level of false positives is also very high. It is also known as proactive technique which contains an anomaly behavior detection technique. Different types of detection and analysis techniques are used before actually performing the heuristic-based detection technique such as weight-based techniques, file-based techniques, rule-based analysis, and signature-based analysis.

There are three basic components of the heuristic-based detection technique:

(1) Data Collection: This component deals with the collection of data whether it is a static analysis or a dynamic analysis. This all depends on the type of the detection technique one is using and also the kind of malware that is found in the code of the system.
(2) Interpretation: Here, the data are interpreted which are being collected in the previous component and then converted into some another form which is mainly the intermediate form.
(3) Matching Algorithms: Here, the behavior of the malware is detected, and the detection techniques analyze the proper behavior of the malware, and then, the matching algorithm is recommended for such malware. The functionalities are recorded, and the malware is tackled.

A proper malware detector is shown in Fig. 7.6 which explains its regular and proper functioning. All the functionalities of every component are shown in the figure, and they work together to detect the malware and analyze it and tackle it.

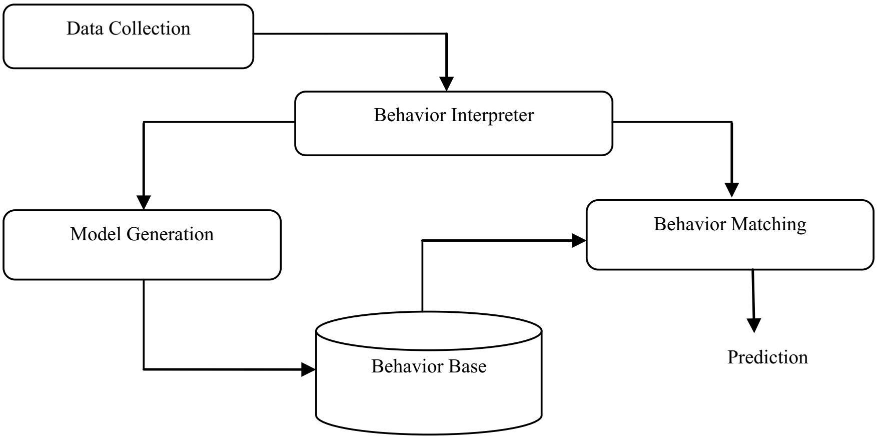


Fig. 7.6 Heuristic-based technique

7.4.3 Specification Based

In the specification-based technique, the applications and the programs are monitored based on their specifications, and then, the system is checked for the normal and the abnormal behavior. The specification-based technique is mainly derived from the heuristic-based techniques. The main difference is that heuristic-based detection techniques mainly uses the techniques like machine learning and artificial intelligence (AI) which mainly detect the valid and the invalid activity of the system. On the other hand, the specification-based techniques look into behavior analysis of the malware that are described in the system specification. Manual comparisons of the normal activities of the system are recorded. The specification-based techniques overcome the problem of false negative by increasing the levels of false negative and decreasing the level of false positive.

Specification-based techniques mainly make a certain set of rules which are mainly considered as the normal set of rules for the proper functioning of the system. Whenever this predefined set of rules is violated, only, then the maliciousness of the program is proved. Thus, the programs that violate the normal set of rules of the system are considered malicious. A detection algorithm is formed by the specification-based approaches which incorporates a considered set of instruction semantics that are used to detect the malware instances in the system. The malicious behavior of the malware is described by a certain set of variables as well as the symbolic constants. The attributes of a particular program are not clearly classified by this proposed algorithm of the specification-based techniques.

Anomaly-based detection is a component of the specification-based detection. It is an intrusion-based detection which mainly detects the network-based misuse of the information and node capture, and the system activity is also monitored here. This technique approximates the needs and the requirements of the applications present

Table 7.2 Differences in malware detection techniques

S. No.	Signature based	Heuristic based	Specification based
1.	The already recognized malware can easily be detected here	In this, the known as well as the unknown malware can easily be detected	It is a step ahead of the both signature-based and heuristic-based methods as it can detect known, unknown as well as new malware in the system
2.	It uses least number of resources as compared to other techniques	The level of false positives is high in these methods	The level of false positives is very low in these methods
3.	The main disadvantage of this technique is that the new malware is not detected in this	The database is updated at regular intervals such that the known and unknown malwares	These methods are not that efficient in the detection of new malware

in the system instead of approximating the implementation of the system. A training system is formed that learns how a valid system works; it notes all the valid behavior of a program or a system, as a whole which is needed to be inspected by the detection algorithm. The main disadvantage of the specification-based technique is that it is very difficult to accurately predict the correct behavior of malicious program in a system. This is mostly impossible to know the valid behavior of a system in all the directions. Table 7.2 discusses the basic difference among the malware detection techniques.

7.4.4 Static and Dynamic Detection

Dynamic approach mainly monitors various executables during the run time and look for the abnormalities in the code execution. Sometimes, one cannot fully detect the malware at the time of the execution because some malware require the trigger conditions or the favorable conditions in order to get activated. Hence, finding malware at execution time becomes a cumbersome task and a resource-intensive process. It becomes difficult to figure out the appropriate environment to run the IoT executables and to test their functionalities completely. Apart from the dynamic analysis limitations, other threats that are prone to IoT devices are MISP (MISP threat sharing), ARM (Advanced RISC machines), PowerPC (Performance optimization with enhanced RISC—performance computing), Spark, etc. MISP is a threat sharing platform acts as an open-source threat intelligence platform also. Power PC is a computer project which keeps on improving day by day developed in 1991 by Apple-IBM-Motorola alliance, and till now, with trademark implementations, it keeps on improving itself. Therefore, providing an environment that meets all the demands and the requirements of the IoT executables in order to get them function properly and correctly is difficult.

In static approach, no execution of the files is done; rather, it analyzes and detects the malicious behavior of the files. The main advantage of static behavior over the dynamic one is that it can observe the malware architecture, and by analyzing, it can take the further steps to stop the malware from corrupting the files. It can look into all the possible execution paths considering the diversity of the malware architecture. It tries to make an efficient approach that can solve the heterogeneous issues other than malware in the IoT devices. Hence, in this way, static approach takes a different way than the dynamic approach in order to know about the malware architecture and its functionalities and what necessary steps should be taken in order to tackle with the existing malware in the IoT device.

7.5 Use Case Example

Several high profile use case examples of malware and viruses have come up which have caused widespread damage to the software architectures as well as the hardware devices. The infamous WannaCry malware which is an example of ransomware has caused several threats to the systems and devices, and it works by encrypting the contents like files and folders of the affected system, and they threaten the users that they will leak the confidential information. Potential destruction to the security system of the devices and data loss is caused by such use case examples of malware. These malware may replicate themselves and spread to the other devices.

7.5.1 Mirai Malware

Malware is a kind of malware which mainly converts the devices present in the network working on Linux into remotely controlled bots that are mainly a part of large-scale botnet network. IP cameras, home routers are the primary targets for the Mirai malware. Thus, malware was first found in 2016 by a malware research group and is one of the major disruptive distributed denial-of-services attacks (DDoS). Mirai is the malware which targets Linux operating systems, and then, they take the control of the Linux operating device and connect it with the remote bots. When the devices are controlled and become a part of a botnet network, then these devices can be used for malicious attacks in the broader network coverage.

IoT devices like home automation devices and IP cameras are the primary target for the Mirai malware. According to a recent report, Mirai malware is one of the most active botnets till date. Mirai malware updates itself with the kind of devices they are attacking, so they have some extended features. They are able to convert the affected devices into the swarms of malware proxies. Hence, through these extended features, Mirai malware is able to attack the devices with the known as well as the unknown vulnerabilities. Crypto-mining has become a common concept of malware these days. The attacker can threaten the system's user to pay the cryptocurrency or

Bitcoin payment in order to prevent the attack from happening. The attacker can use the victim's system electricity as well as hardware of the system to earn the cryptocurrencies by using the Mirai malware. Several new ways are being experimented that how IoT botnets can also be used to make online money by attacking several users.

7.5.2 Reaper

Reaper was basically made as antivirus software which would stop the transmitting of a Creeper virus. Its main purpose was to move across devices and look for the self-replicating Creeper program and delete it. Reaper was a worm initially designed to delete as many instances of Creeper program as possible. Reaper has evolved in the strategies and computer hacking techniques which may break into the devices instead. It not only guesses the passwords of the systems these days but it has found out the flaws in the code of these insecure vulnerable devices, and hence, hacking into such systems become easy, and the devices are easily compromised. Hence, Reaper exploits numerous vulnerabilities of the IoT devices, and it becomes even a bigger risk for the devices.

Reaper is the malware which is also called as an IoT roop. Large chunks of code were taken from the Mirai malware, and several improved changes were done in the code to make the attack more effective then that botnet was called as IoT roop which is basically Reaper. Reaper is an improved version of Mirai malware such that it has better functionality features than the Mirai malware. Reaper compromises a smart IoT device way quickly than a Mirai botnet. There are very severe effects of Reaper as it can easily bring down the whole infrastructure and architecture of the victim device very easily and very quickly. Mirai only targets the default username and passwords of the victim device, while Reaper targets several vulnerabilities of a system which may include different makers such as D-Link, Linksys, Netgear, and Internet-connected surveillance cameras. Using a botnet, the attacker can make some changes in its features, and then, the malware code becomes more devastating.

7.5.3 Echobot

Echobot is a new variant of malware, and it was first discovered in the beginning of the year 2019. It is like a variation of Mirai but far more dangerous, as it uses a large number of malicious scripts, and then, it spreads itself. At the starting, it exploited around 18 vulnerabilities of the victim's system, but now, it can exploit up to 26 scripts. Echobot has launched attacks against a large number of IoT devices, and it has improved itself up to a level that it can exploit 50 vulnerabilities till now. It also led to a rise in command injection over the HTTP which impacted around 34% of the organizations across the world.

Echobot takes the advantage of the unwanted smart IoT devices, and then, these bots use these existing vulnerabilities of the devices and harm the applications residing in the system. There was another Echobot like botnet which was called Emotet which also became active at the time when Echobot was discovered. Hence, these both bots share some specific design features.

7.5.4 Other Potential Attacks

There are a large number of botnets existing in the world, and some are even difficult to trace and to know their feature specifications to tackle them. These botnets are able to discharge an enormous amount of spam to deliver a particular amount of payload. Through these spam, these botnets are able to get the users to perform various malicious tasks. Some of these botnets are discussed below.

EMOTET: Emotets are used for the stealing of emails from the mailboxes of the victims. By using Emotets, attackers can also fool the recipients into opening the spam, and the important and confidential information can be accessed by these attackers. These attackers can also steal the credentials of the users which may help them in taking control over the emails of the users, and then, they can use them for illegal purposes.

GAMUT: Gamut is a type of botnet which also works like the Emotet and specializes in the spam emails. The first thing that it does is to develop a stable relationship with the victim user or the target machine such that it gains trust of the victim in order to steal their emails. This trust is gained through online dating request or some kind of job offer with favorable conditions.

NECRUS: Necrus is used to launch a ransomware attack, and it is used to mainly threaten the users with a ransom amount. It also performs some digital extortions. According to a research done by Cisco, Necrus is till at a developmental stage and can create havoc in the system once launched. Hence, devastating attacks can be launched by Necrus once installed into the system.

MOZY BOTNET: This is a new botnet that has come up in the IoT devices since its discovery in 2019, and it has a code overlap such that it also exists as a Mirai variant in several places. It accounted for almost 90% of the total IoT traffic in October 2019–June 2020. Mozy flooded the market with different dwarfed variants and did not removed the competitors if the market. The attacks were 400% higher in June 2020 than the combined attacks of other botnets in the previous two years.

7.5.5 Pegasus (2021)

Pegasus was initially discovered in 2018 developed by the Israeli firm called the NSO groups which were a spyware mainly developed for the android and iOS systems mainly smart phones. This spyware is capable of reading the text messages on the system, tracking the calls ingoing and outgoing, collecting the username and passwords, location tracking, accessing device's microphone and camera, and hence harvesting and collecting the information from all the acquired assets of the device. Pegasus spyware has got the nationwide attention and was called as the most sophisticated mobile devices attack.

This attack is still prevailing and is at its peak when it was able to hack the smart phones of several political leaders of the Indian govt. as it updated itself with the recent versions of iOS smart phones. It can easily enable the keystroke monitoring mechanism of all the communications from the smart device such as texts, emails, and Web searches. At the time of a Pegasus attack, the smart phone acts as a surveillance device for the attackers, and they can easily access all the important information present on the device.

Hence, the abovementioned botnets like Mirai, Echobot, Reaper, Emotet, and Mozy Botnet are very harmful and dangerous attackers to the IoT devices connected over the Internet. As these IoT devices communicate online, the threats also increase. So, there is a need to improve the security systems of the devices. Better detection strategies, analysis programs should be installed in the devices in order to protect them from the attackers. The users should also be attentive while performing a task or opening a link or while sending some confidential information or putting a safe and secured passwords for their systems. The graph given in Fig. 7.7 shows the increasing IoT attacks in the recent years. Quarterly, analysis report is given by from 2018 to the first two quarters of the year 2020.

The top malware that come up according to the number of devices affected globally are XMRig, JSEcoin, Dorkbot, Trickbot, etc. XMRig had a global impact of around 7% of the systems around the world. It is open-source software which is used for the mining process of the cryptocurrency, and it was first discovered in 2017. The

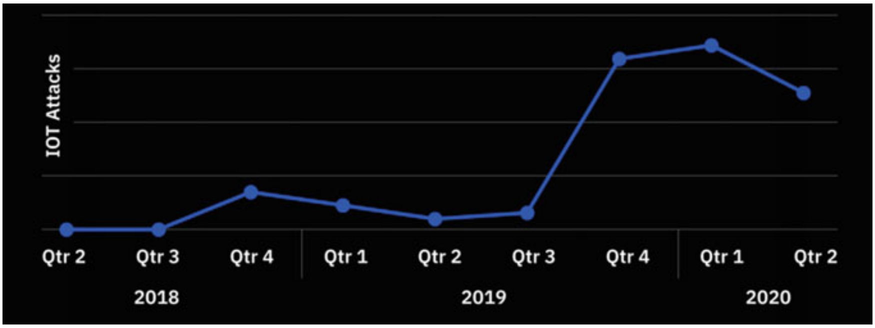


Fig. 7.7 Increase in IoT attacks

second most dangerous malware is JSE coin which also has a global impact on 7% of the systems. It is basically a JavaScript, and then, it can easily be embedded in the Web pages. The miner runs with the help of JSE coin, and it can run directly on the browser in the exchange of the ad free experience of the Web site. Sometimes, it acts as an in game payment of cryptocurrency and several other incentives.

On the third place comes Dorkbot which has impacted 6% of the systems globally till now. Dorkbot is an IRC-based worm which is designed for the remote code execution by its remote operator. It can download some of the additional malware such that they can infect the system. Trickbot is another dominant banking Trojan mainly used for threatening the user into paying some ransom. It constantly gets improved, updated with its new features and capabilities as well as the distribution vectors. That is why Trickbot is a customized malware and has very flexible features that can be used for distributed systems and for multi-purpose tasks. Hence, this becomes easy for Trickbot to get into the Web sites and programs.

There is a list of the most affective malware for the mobile computing taken from the previous year data depending upon the number of devices affected. Lotoor is a hack tool which exploits the vulnerabilities of the android devices in order to gain the privileges like username and passwords of the compromised android smart phones. Another one is android bots which is an adware which targets the android devices which get the data about IMEI number of the devices, its GPS location and some other confidential information about the device. It allows the installation of the third-party applications and various shortcuts on the mobile devices. Triada is another backdoor malware which grants the android users various free privileges which can get downloaded and get embedded into the systems.

7.6 Research Opportunities in Malware

Malware is growing these days at very high rate, and in the last decade, a very impressive progress has been made by the antivirus software mechanisms. Although several amount of harmful issues have been discussed and addressed adequately in the previous sections but a lot of research opportunities are still there in this field. In today’s modern world, the static, dynamic, or even hybrid methods don’t work on the unknown or novel signatures of the malware existing in the system. Virtual environments are made by the antivirus software to run the malware and see how it behaves. But, these days, the virtual environments have become very less effective as the attackers are always one step ahead in concealing of the malicious activities at a high level. Hence, all the efforts are made to make a high level, multi-layered system such that the antivirus systems are not able to identify the true functioning of the malware and to know which is the family of the malware and several other things. There are a lot of problems that the antivirus software is dealing with these days like:

(i) Lack of real-word representative datasets of affective malware
(ii) Very low generalization and the detection of the malware

(iii) Scalability issues in antivirus software.

There is a need of effective, efficient, and comprehensive techniques and countermeasures which can use several machine learning, deep learning techniques, data mining methods, and adaptive measures. Several anomaly-based methods which use behavioral analysis schemes which are mainly designed to investigate the malware on the basis of the behavioral features of the malware and what are the malicious activities done by the malware. These methods can help in minimizing the errors and improving the results. They may also help in decreasing the false alarm rates of the malware. Some of the research fields are discussed below.

7.6.1 Advanced Machine Learning (AML)

In today's times, several quintessential antimalware depend on the explicit information about the malware, expert domain knowledge, advanced set of models, and architectures, and hence, they are prone to the low overall reliability and several other factors. These advanced machine learning techniques try to know the attackers by imitating them on the basis of contexts, content, etc., rather than making some advanced architectures or models or systems. A lot of work can be done in the AML antimalware systems and techniques beside their advantages over the malware and viruses. Several other techniques can be somehow connected to the AML techniques like the open set recognition paradigm, residual deep learning, data mining, and knowledge database which can be used feature extraction, learning, classification, selection. These all things can help in determining the relationships that exist between the malware and inside the malware sections.

7.6.2 Mobile Device Malwares

Smart devices that are connected over the Internet are increasing at an exponential rate, and mobile malwares are also increasing against them. Antimalware systems are very difficult to install in the smart devices because of their complex implementations, high computing costs, complex analysis, etc. This is why, real world, lightweight mobile antivirus is used in the smart devices, and hence, Bayesian classification techniques are a good place that can be researched further in this field. The performance of the mobile antimalware can be enhanced from the inbuilt sensors present in the smart devices. Other than the software malware detection, another field that can be explored is the hardware malware detection in the mobile devices, and the removal of hardware malware is a serious issue. Preventive and effective countermeasures can be adopted for the smart devices antimalware. The app developers follow a set of rules that abide the security and the privacy policies. The dubious apps must be removed from the mobile devices, and the users should also look to use the superior apps and only install the trusted apps.

7.6.3 Graph-Based Malware Analysis

The graph-based malware analysis techniques are the most conventional antimalware techniques and dominant these days and very effective. Conventional antimalware highly disregards the learning processes and the underlying and developing relationships between the malware samples and the variants as well as the contextual information. Several graphs are used for the relationship representations like call graphs, control flow and data graphs, and dependency graphs, and they can be easily used for the constantly evolving malware as they can easily track the work and evolvement of the malware. There are several issues that need to be dealt with in the graph-based techniques such as noise, computational costs, and real-time detection. Some of the research fields that can be looked into are multiple directed and the undirected graphs, spectral clustering, kernel learning, heterogeneous networks, dynamic graph mining, deep learning graph convolution kernels that are used to capture the contextual and the structural information.

7.6.4 Defense in Depth Malware

Defense in depth malware methods contain the different levels and lines present in its architecture. These types of methods are expected to be the most robust software which contain more than one defense techniques such that if the one level is breeched, then there is another level to be looked into. Every system in this is divided into different levels such as if there is a power grid system, then it will include communication framework, components are divided into the lowest, intermediate, and the high levels of the architecture. Active defense systems are used and have enhances their complexities as they make the scenario of a malware attacking the system, and then, the developers make the countermeasures. In adaptive defense, the system evolves and updates according to the environment with the novel features. Adaptive systems require very fast, automated unsupervised learning which must be effective. IoT devices are being used everywhere, and hence, the cyberattacks are also increasing on them despite the security systems used by these IoT devices. IoT cybersecurity is a new research domain that can be quite challenging.

7.6.5 Bio-Inspired Malware

Several bio-inspired malware can be used to overcome the traditional antimalware techniques. Some bio-measures are such as biological evolution, biological immune system, genetic algorithms, and swarm intelligence. These techniques are scalable, lightweight, resource constrained, etc. Adaptive measures use feature extraction and classification that can easily be enhanced accuracy. The bio-inspired methods use the objective functions in order to discriminate a system which is under attack by a malware or if the systems keeps malfunctioning or failing which may also help with the strengthening the security. Bio-inspired malware can be combined with the neural networks which are one of the most promising research options in the antimalware.

7.6.6 Malware Education

The humans are the weakest links where the malware can directly attack, and hence, the cybersecurity is very important to educate the people about the malware safety to the people. In the educational institutions, the effective measures about the malware are taught to the people, and there are several courses related to this at both graduate and the undergraduate levels. There is a shortage in the courses about malware, and they are in limited colleges and universities, so there is a shortage in the fundamental topics. Many research oriented, academic courses which deeply rely on text books are offered to the interested people. Training camps, workshops are held by the major corporate companies and organizations which are mainly for the general public. Online free courses with the certificate training courses are used. Interdisciplinary research methods are the state-of-the-art analysis methods are used in the fundamental methods and developmental methods which have the contributions from the deep learning, computer engineering, machine learning, etc.

7.6.7 Big Data Malware Analysis

The demands of the big data in the field of malware analysis are increasing day by day and are steadily expanding. There are a lot of big data malware challenges that the practitioners these days are working on such as volume, velocity, variety, veracity, and value. Volume includes collecting, aggregating, data cleaning, and data compressing. Velocity includes the real-time online training, processing, learning, and streaming. Value includes the machine learning-based malware analysis and deep learning. Variety includes several kinds of heterogeneous data learning and embedding of multi-view data. Veracity includes learning through contradiction and the unreliable data. The future research in this field includes feature selection techniques, feature engineering, low-rank matrix approximation, graph theory, adaptive feature scaling, and fuzzy clustering. Several efforts are made to develop the knowledge of the pros and cons and use the antimalware with the right techniques.

7.6.8 Deception Antimalware Techniques

These deception techniques mainly lure the adversaries by misleading them into the false information. Honeypots malware is used against the deception malware which are of two kinds, namely client and server. Honeypots are used to prevent the denial-of-service attacks and to eliminate or reduce the false positives from the system. Several advanced polymorphic malware identify the honeypots in the system and try to alter their behavior such that the honeypots deceive themselves. These honeypots are easily exploited by the attackers which undermine the several parts of the honeypots. Advanced honeypots schemes should be used such as shadow honeypots such that the security can be put on the whole organization of systems which are under attack. Another thing used here is the moving target techniques such as dynamic platform methods (DPMs). DPMs are a complicated application which can be present on the varying platforms, and hence, not only, one adversary can evade the DPMs. Less efforts are being made to the development of the articulated attacks with the up gradation of the deception methods.

7.6.9 Botnet Countermeasures

Botnets have become an interesting area, and several new detection and defense architectures are coming up and being proposed. There are a lot of issues in the botnet countermeasures such as the problems in the testing devices which test the botnet samples in real-life scenarios and with different datasets. Other difficulties include the quantitative evaluations that help in comparing the botnet defense which is due to the privacy problems and the data sharing concerns. Botnets like IoT bots and social bots are continuously increasing, and they can only be controlled if some good technical as well as non-technical measures are to be made and devised. The technical factors include Internet service providers, while the non-technical factors include the establishment of a distributed environment, some legal issues and some poor awareness of the users and other people.

7.6.10 Malware Advertisements Learning

Adversaries which adapt machine learning techniques are continuously being used in order to achieve the effective malware defenses. Such adversaries are not effective in the situations where the malware is trying to impact the outcomes of the concerned system. Many machine learning countermeasures lack the robustness in them against the adversaries. Attackers can include the poisonous samples inside the effected system through online or adaptive training which aim at decreasing the accuracy of the malware counter measures in the testing phase. A comprehensive study is done for the malware and viruses depending on the capabilities of the attacker as well as the features which can be modified up to what extent such that the malware detection techniques are made up to that point. It is a very difficult task to make the anti-malware software that are robust in nature for the malware adversaries. Hence, researchers need to explore the malware adversaries and how they can be tackled, identified, detected, and hence, there is a need to train and test several levels of malware. Hence, a technique that robust in nature is required in these days.

A lot of work needs to be done in the field of IoT malware, and researchers have found some of the optimal solutions, but still there is need of a proper secure system which can detect the unknown viruses as soon as they attack the device. Several high-level security measures need to be taken such that they have a strong upper hand than these attackers. Other fields like data analytics tools for the collection of data should be explored as this collected data needs to be secured from the attackers. Hence, a lot of work need to be done in different fields to stop the attackers from attacking. A strong uphold of the security systems should be there which can protect the systems.

References

Akhtar Z (2021) Malware detection and analysis: challenges and research opportunities, Jan 2021, pp 1–10

Choo KKR, Yan Z, Meng W (2020) Editorial: blockchain in industrial IoT applications: security and privacy advances, challenges, and opportunities. IEEE Trans Ind Inform 16(6):4119–4121. ISSN: 1551-3203

Damodaran A, Di Troia F, Visaggio CA, Austin TH, Stamp M (2015) A comparison of static, dynamic, and hybrid analysis for malware detection. J Comput Virol Hack Tech 13:1–12

Ngo Q-D, Nguyen H-T, Le V-H, Nguyen D-H (2020) A survey of IoT malware and detection methods based on static features. ICT Express 1–7

Tahir R (2018) A study on malware and malware detection techniques. Int J Educ Manag Eng (IJME) 2:20–30

Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M (2020) IoT privacy and security: challenges and solutions. Appl Sci

Tewari A, Gupta BB (2018) Security, privacy and trust of different layers in internet-of-things (IoTs) framework. Future Gener Comput Syst

Tiwary A, Mahato M, Chidar A, Chandrol MK, Shrivastava M, Tripathi M (2020) Internet of things (IoT): research, architectures and applications. Int J Future Rev Comput Sci Commun Eng 4(3):23–27. ISSN: 2454-4248

Wazid M, Das AK, Rodrigues JJPC, Shetty S, Park Y (2019) IoMT malware detection approaches: analysis and research challenges. IEEE Access 2

Zhang Z-K, Cho MCY, Wang C-W, Hsu C-W, Chen C-K, Shieh S (2014) IoT security: ongoing challenges and research opportunities. In: 2014 IEEE 7th international conference on service-oriented computing and applications

Chapter 8
IoT Network Used in Fog and Cloud Computing

Umang Kant and Vinod Kumar

8.1 Introduction

As we witness tremendous start-ups and ventures happening over the Internet, there is enormous growth in the generation of data. To manage all the data over the Internet and establishing their relationship with the connected devices, the need arises of effective IoT frameworks and networks to manage all the data being stored over the nodes in cloud, fog, or edge computing. As discussed above, since almost all the business is happening over the Internet these days, it is evident that now these businesses, their respective environments including the people involved and the data generated, cannot thrive without IoT. IoT has given unprecedented connectivity options to the entrepreneurs and various industries to manage all the data effectively over a single platform and be it in the field of health care, transportation, agriculture, marketing, manufacturing, and energy to name a few. IoT in cloud and fog computing has extended public cloud services by offering a third-party access to the platform and infrastructure. This section includes brief discussion on IoT, cloud computing, and fog computing.

8.1.1 Internet of Things (IoT)

Over a period, different organizations have proposed different definitions and architecture of IoT; hence, there is no clear definition for same. The work of various researchers can be discussed to analyse and understand the concept of IoT. IoT can be seen as an umbrella that covers different categories of smart devices, which include wireless sensor networks, Internet-connected wearable devices, low power embedded

U. Kant (✉) · V. Kumar
Delhi Technological University, Delhi, India
e-mail: umangkant_2k20phdco03@dtu.ac.in

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_8

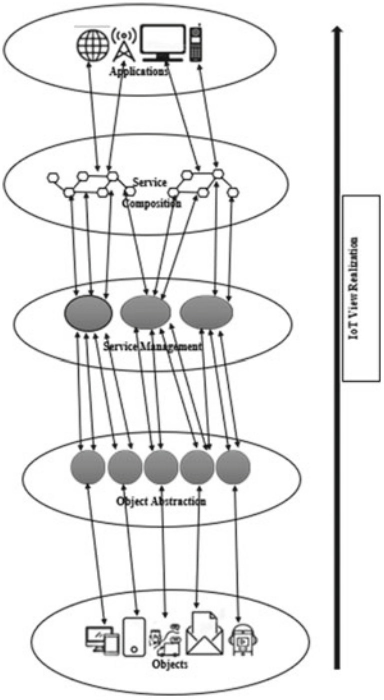


Fig. 8.1 Overall view of IoT Paradigm

systems, RFID-enabled tracking systems, smart homes, connected vehicles, and many more (Ashton 2009). Figure 8.1 depicts the overall IoT paradigm.

Yun and Yuxin (2010) have researched on the architecture and key technology of IoT along with the interpretations of applications of IoT. The application of IoT in smart grid is emphasized by the authors. They have proposed a definition which includes terms like, 'smart grids', 'smart power grids', 'IoT infrastructure', and 'power engineering computing' to refer to IoT. Mei et al. (2019) have proposed some definition of IoT and have included terms like 'global infrastructure', 'global network infrastructure', 'worldwide network' to refer to IoT. The common aspect in the proposed definitions is that the authors have built a bridge between the virtual and physical objects. These objects support communication and data processing. Chen et al. are also concerned with the high implementation cost of IoT due to the integration of data and protocols. Hence, they have emphasized on the requirement of an open and generic architecture of IoT. In Ray (2016), P. P. Ray has done a survey on various IoT architectures. The author has discussed about the (i) *IoT functional blocks* (Fig. 8.2), (ii) *utilities of IoT*, (iii) *IoT supported technologies*, (iv) *hardware platforms*, (v) *wireless communication standards*, (vi) *cloud solutions*, (vii) *application domains* (Fig. 8.3), and (viii) *domain specific IoT architectures* (Fig. 8.4). If we discuss in brief, IoT is conceived to integrate small communicating devices with the parameters we aim of monitoring over the Internet. The focus of IoT is to

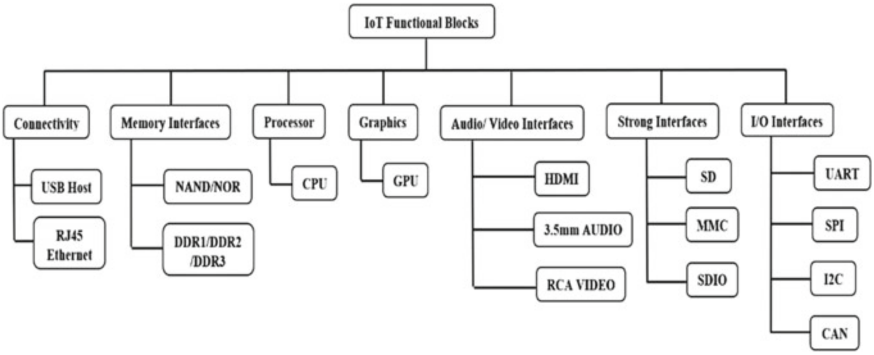


Fig. 8.2 IoT functional blocks (Ray 2016)

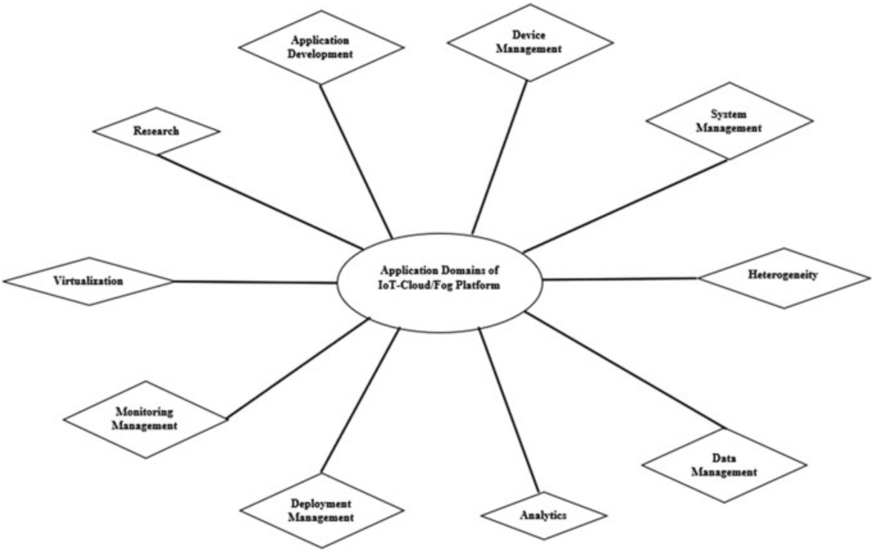


Fig. 8.3 IoT application domains using cloud and fog paradigm (Ray 2016)

connect things or devices to the Internet, so that they are in constant contact of users which can access, monitor, and control then remotely (Xia et al. 2012).

8.1.2 IoT Networks and Architectures

IoT networks deal with two core components: (i) *sensors* and (ii) *actuators*. Sensors are used to collect the data in context, and actuators collect commands to control and monitor the environment. Latest research and developments in the networking

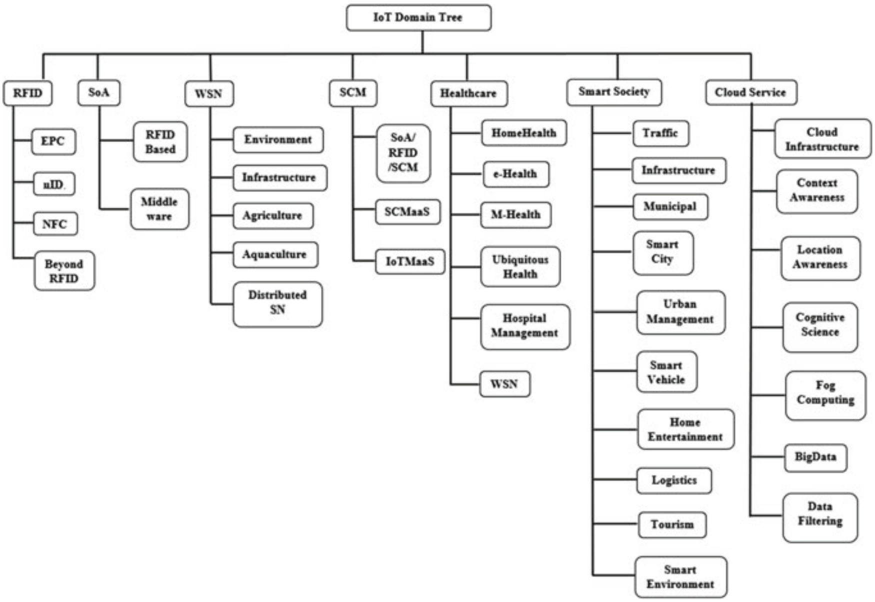


Fig. 8.4 Domain-specific IoT applications (Ray 2016)

and cloud infrastructures have enabled the researchers to investigate and discover the requirements of IoT network virtualization. IoT network virtualization deals with the amalgamation of cloud/fog computing, IoT, and software-defined networking (SDN). These IoT networks incorporate cloud infrastructure by allowing users to run application on cloud or fog platforms. The benefits of these IoT networks are (i) *simplicity in managing and processing data*, (ii) *eliminating the requirement for infrastructure advancement*, (iii) *reduction in processing and maintenance costs*, (iv) *better smart device communication*, and (v) *efficient use of application programming interfaces (APIs)*. These IoT networks also be extended to fog computing paradigm. These systems produce massive amount of application associated data which is required to be efficiently analysed and processed. This large amount of data is posted to the cloud as it is difficult to manage this quantity of data otherwise, though cloud also has its limitations. These limitations can be overcome by shifting to new paradigm of fog computing which includes an additional layer for data processing. After data processing, this layer transfers the results and related information to the cloud. Fog computing is a technology which is introduced to bridge the gap between the IoT devices and remote data centres, which in turn enables large numbers of advantages such as reduced bandwidth, reduced latency, and increased security. Although both cloud and fog computing have their respective advantages, the security and privacy issues still challenge the overall implementations of these IoT networks. The devices associated with the cloud/fog-based IoT network communicate through gateways access the various services, tools, interfaces, and resources provided by the network. These services can be coordination, connection, subscription, and discovery services. Application development tools and application programming interfaces provide means of efficient communications. Networks provide processing, network, and communication resources as well. Implementation of IoT networks is required to maintain the IoT network protocols. In brief, these protocols can be listed as (i) *Bluetooth*, (ii) *BLE*, (iii) *ZigBee*, (iv) *Z-Wave*, (v) *6LoWPAN*, (vi) *Thread*, (vii) *HaLow*, (viii) *2G, 3G, 4G, 5G*, (ix) *LTE*, and many more. The implementation of IoT networks faces various security issues, threats, and challenges. These security concerns include the following: (i) *misconfiguration*, (ii) *insecure APIs*, (iii) *unauthorized access*, (iv) *account hijacking*, (v) *external data sharing*, (vi) *limited ability to monitor resources*, (vii) *malicious insider threats*, (viii) *cyber-attacks and denial of service attacks*, (ix) *data leakage, data loss, and data breaches*, (x) *data confidentiality*, (xi) *legal and regulatory compliance*, (xii) *cloud protection*, (xiii) *insecure access control points*, and (xiv) *regulation, compatibility, and bandwidth*, among other issues.

The emergence of the software-defined network (SDN) has raised awareness about the various advantages of this paradigm. Instead of making forwarding decisions, network devices communicate with a network controller, which acts as a central hub. Different protocols are used to communicate with the network devices. OpenFlow is a software development kit (SDK) that enables network devices to establish a secure connection to an SDN controller (Gonzalez et al. 2016). It also enables quick reaction to security threats. The OpenFlow flow rules can be dynamically modified to adapt to different network conditions. It was initially built to run on production networks. The advantages of utilizing SDN techniques in IoT environment can make the IoT much easier to manage, protect, and reconfigure.

The IoT networks can be realized by incorporating dedicated architectures. Oliver et al. (2015) by their research contributed a software-defined networking (SDN) architecture with the aim to tackle security concerns in IoT, to enhance security policies exchange and deployment control domains. Their work has been inspired by the existing network access control and security techniques. SDN works as a strategy to expand the functionalities of the IoT network, which in turn reduces costs and hardware complexities. This architecture has three layers as shown in Fig. 8.5, each layer responsible for specific components and tasks (i) *infrastructure layer* consists of various required network devices such as switches, virtual switches, access points, and routers, (ii) *control layer* consists of SDN controllers such as POX, NOX, MUL, Beacon, and Floodlight, and (iii) *application layer* incorporates functions for configuring the SDN such as access control, traffic and security monitoring, energy efficient networking policy, and network management.

8.1.3 Cloud Computing and Its Integration with IoT

Cloud computing can be understood as a concept which aims to provide quality service, flexible infrastructure, configurable software facilities, and dependable computing environments for the market and end-users. The term cloud computing

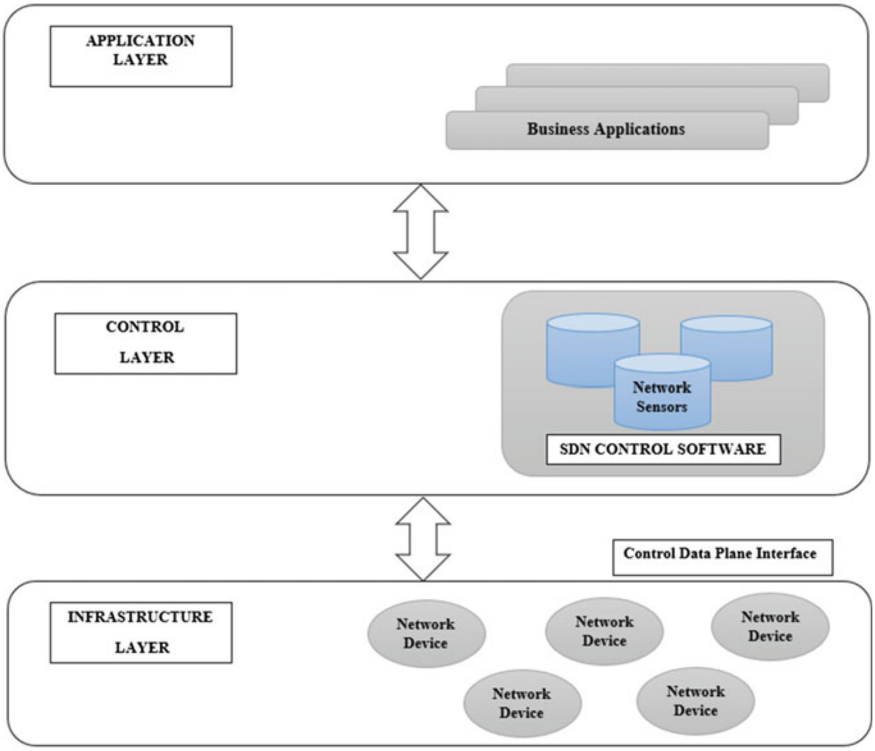


Fig. 8.5 Software-defined networking (SDN) architecture

was coined in the year 2007. Wang et al. (2010) have proposed a detailed definition of cloud computing stating '*A computing cloud is a set of network-enabled services, providing scalable, quality of service guaranteed, normally personalized, inexpensive computing infrastructure on demand, which could be accessed in a simple and pervasive way*' (Wang et al. 2010). The client companies or end-users are given the computing platforms or infrastructures from the computing clouds to deploy and run their applications on it. The computing clouds provide the complete access to the hardware–software and data resources in turn providing the further services in an efficient manner. The functional facets of cloud computing, depicted in Fig. 8.6, are termed as *Hardware as a Service* (HaaS), *Software as a Service* (SaaS), *Platform as a Service* (PaaS), and *Data as a Service* (DaaS). With the collaboration and support of HaaS, SaaS, and DaaS, the cloud computing can cater to another service for user which is termed as *Infrastructure as a Service* (IaaS) and *Anything as a Service* (AaaS).

The pictorial representation of cloud and IoT basic integration is depicted in Fig. 8.7 (Atlam et al. 2017). Cloud computing is distinct due to its exceptional features such as (i) *user centric features*, (ii) *service provisioning*, (iii) *guaranteed quality of service*, (iv) *autonomous environment*, (v) *scalability*, and (vi) *flexibility*,

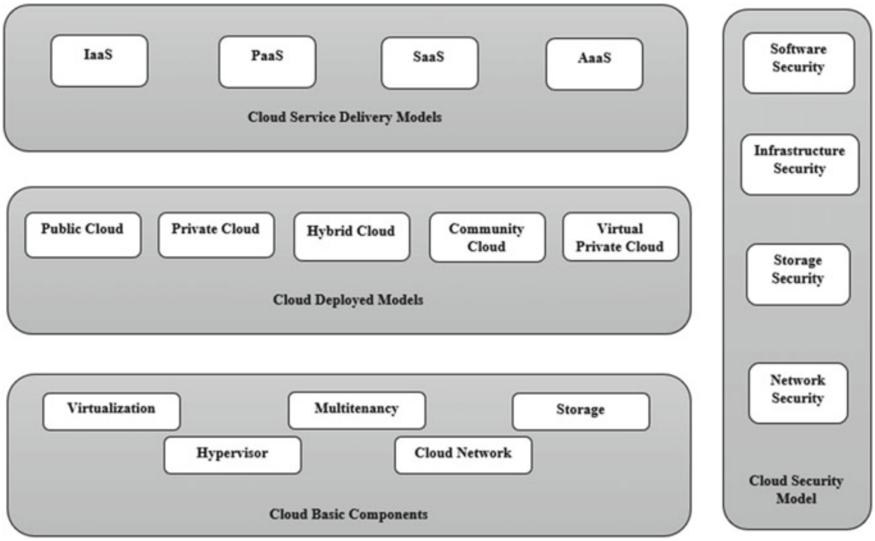


Fig. 8.6 Functional facets of cloud computing

among others (Aazam et al. 2016). Although there are some limitations which do not allow cloud computing alone to manage intensive computations and mass storage, these limitations have motivated the researchers to integrate the IoT with cloud in the form of mobile cloud computing (MCC). This integration is aimed to enable mobile devices and make them resourceful with more computational power, storage, memory, energy, etc.

MCC can be understood with respect to (i) *infrastructure-based mobile cloud*: here the hardware remains static, and (ii) *ad-hoc mobile cloud*: hardware is not static. MCC has been depicted using Fig. 8.8. Cloud computing and IoT are related to each other with respect to the same characteristics such as (i) *service on Internet platform*, (ii) *storage on Internet platform*, (iii) *applications on Internet platform*, (iv) *energy efficient Internet platform*, and (v) *computationally capable on Internet platform.* The detailed discussion of this hybrid platform is covered in Sect. 8.2 of this chapter.

8.1.4 Fog Computing and Its Integration with IoT

As discussed above, cloud computing has seen an exponential growth in its usage and application in various real-time problems, but this technology does suffer from few shortcomings such as (i) risk of data confidentiality, (ii) *Internet connection dependency*, (iii) *security vulnerability*, (iv) *data mobility*, (v) *latency issues*, and (vi) *data*

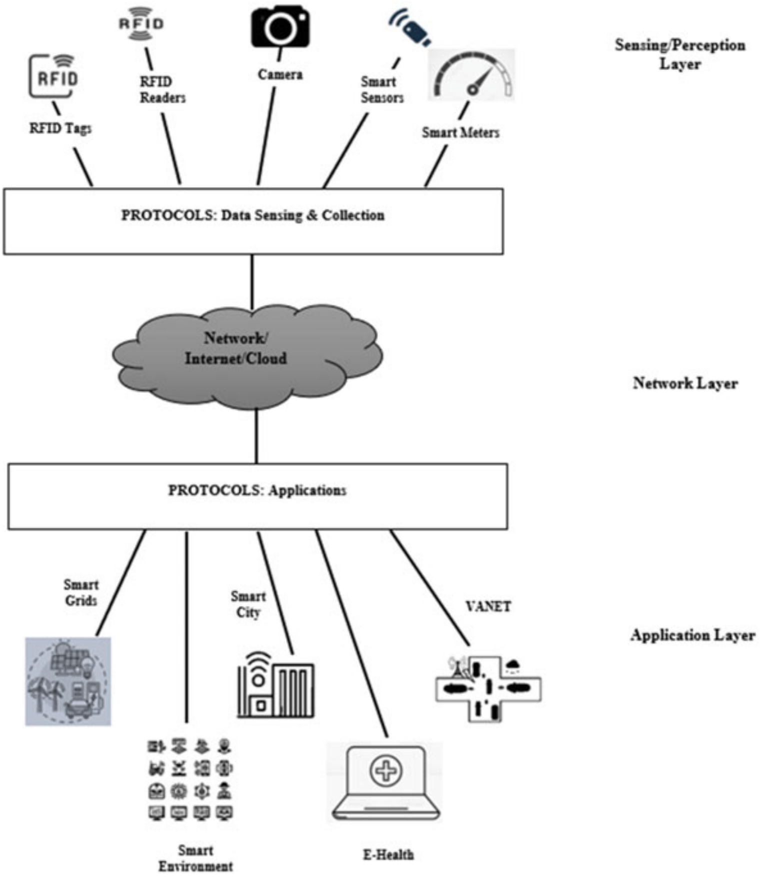


Fig. 8.7 Cloud and IoT integration

mobility, among others. Fog computing can be employed to overcome these limitations related to cloud computing. From the core to the edge of the network, fog computing paradigm can be counted as an extension of cloud computing paradigm and is intended to enable computing right at the edge of the network (Yi et al. 2015). Concepts such as mobile cloud computing (MCC) and mobile edge computing (MEC) tend to overlap with fog and edge computing (Bonomi et al. 2012). This is because the definitions of fog and edge computing are still debatable and overlapping to some extent. MCC, as discussed in the above section, refers to such infrastructure where data collection, storage, and processing occur external to the mobile devices. Since MCC applications extract the processing power and data resources from mobile devices to the cloud, they cater to not only smart mobile phone users but also various mobile service subscribers. In contrast to MCC, MEC refers to the cloud server functioning right the edge of the mobile network. Though fog computing can be seen as the amalgamation of both MCC and MEC, but it still has distinguished features with

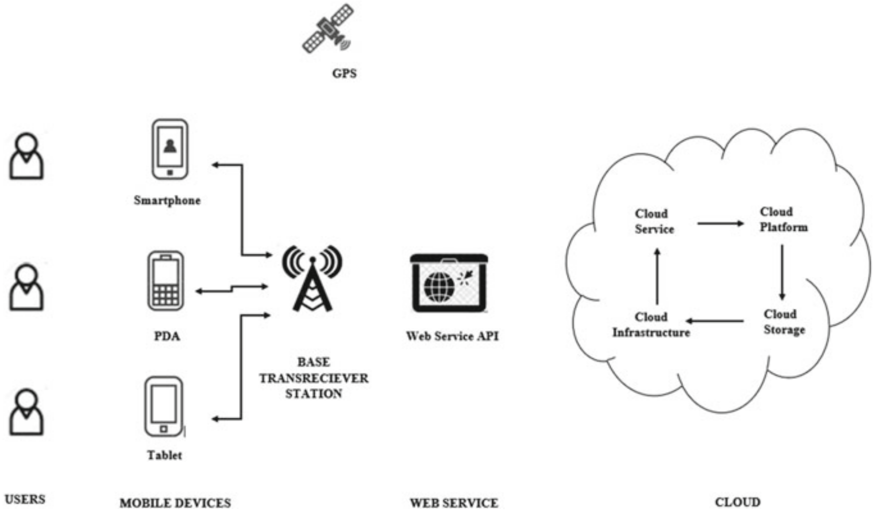


Fig. 8.8 Mobile cloud computing (MCC) architecture

respect to IoT. Edge computing, which in contrast to cloud computing, communicates with the edge data centre located near the device. It leaves the secondary jobs to cloud. Now, this edge computing is considered as a subset of fog computing as fog computing is accountable for managing the data, i.e. it is responsible for identifying where the data has been generated and where it has been stored. Fog computing network is a virtual platform which manages the connections between the cloud and the edge devices, as depicted in Fig. 8.9.

Machine-to-machine (M2M) communication is performed in the first level of fog as shown in the figure. This level is also responsible for filtering the data collected locally and eventually passing the filtered data to the above layers. Human-to-machine interaction (HMI) is achieved in the second and third levels along with M2M. As we move above the infrastructure, the higher levels provide broader geographical coverage and scaling, hence achieving the fog localization. Eventual global coverage is enabled by the cloud acting as the data warehouse for data collected over the period of time which is to be eventually used for data analysis. The key features of fog computing are as follows: (i) *reduced network load*, (ii) *mobility support*, (iii) *context awareness*, and (iv) *absence of single defective point*. The integration of fog computing with IoT is done with the aim of providing localization from fog computing and global centralization from cloud computing. The localization feature in turn enables low latency as well as context perception. Latest technologies and applications like data analytics, predictive analytics, and big data involve fog localization and cloud globalization. The detailed discussion of this hybrid platform is covered in Sect. 8.2 of this chapter.

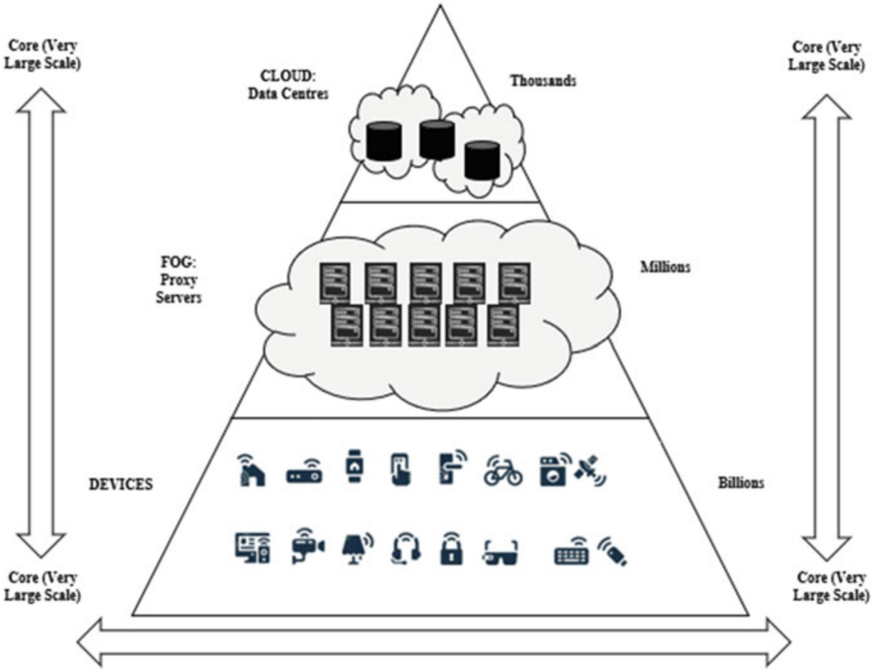


Fig. 8.9 Fog computing architectures

8.1.5 Comparison Between Fog Computing and Cloud Computing Paradigms

As discussed in the above section, fog computing is quite similar to cloud computing, but there are some parameters on which both differ (Saharan and Kumar 2015). This section discusses these comparisons in a brief and tabular form (Table 8.1).

The above table highlights the key differences between the two technologies to make the readers understand that though similar, both are not the same, and fog computing should not be seen as a replacement of cloud computing as both cater to their respective area of expertise. In fact, fog computing should be seen as an extension of cloud computing with few extra characteristics for both the service end and user end.

Table 8.1 Comparisons between fog and cloud computing based on different parameters

S. No.	Characteristics	Fog computing	Cloud computing
1	Latency	Low	High
2	Security, vulnerability	More secure, low	Less secure, high
3	Delay Jitter	Low	High
4	Locations of server nodes	At the edge of network	Within Internet
5	Location awareness	Yes	No
6	Client–-server distance (hops)	Single hop	Multiple hops
7	Geographical distribution	Densely distributed	Centralized
8	No. of server nodes	Large	Few
9	Connectivity	Wireless	Leased line
10	Real-time interaction, mobility	Supported, supported	Supported, limited support
11	Advantages	Dense geographical distribution, maintaining data closer to users, enhanced mobility, support for IoT, better storage space, extension of cloud, integration with various applications and services, bandwidth	Mobility, better collaboration, backup and recovery, storage capacity, low maintenance
12	Limitations	Complexity, security, power consumption, authentication, maintenance	Technical glitches and issues, security and privacy issues, data location, data filtering and segregation, data lock-in
13	Applications in IoT	Real-time analytics, connected and linked vehicles, smart grids, smart cars, etc.	Online data storage, backup and recovery, big data analysis, testing and development, antivirus and e-commerce applications, education, health care, e-governance, entertainment, etc.

8.2 Implementation of Fog Computing and Cloud Computing Using IoT

This section is dedicated to detailed discussion on the implementation of cloud and fog computing using IoT paradigm. Though brief discussion has been covered in introduction section, but it is required to have a detailed overview on the integration of these technologies.

8.2.1 IoT Networks Used in Cloud Computing

Researchers have witnessed an exponential and independent growth of both cloud computing and IoT. Though different, both these technologies have some characteristics which are complementary to each other. These characteristics are as follows: (i) *displacement*, (ii) *reachability*, (iii) *components*, (iv) *computational capabilities*, (v) *storage*, (vi) *role of Internet*, and (vii) *big data.* These characteristics are discussed in Table 8.2. These characteristics have inspired researchers around the world to integrate the two and implement one using the other to extract the benefits of both at a single platform with respect to the application. This integration has led to the term c*loudIoT* (Botta et al. 2016).

IoT can take advantage of the unlimited virtual resources and capabilities of cloud such as processing power, communication, and storage, to compensate for its technological limitations, and also cloud can act as intermediary layer between real-life things and applications, hiding the complexities and functionalities. Vice versa, cloud can gain value from IoT by expanding its extent to real world in a better distributed manner so that real-life application can be catered by cloud as well. The main drivers and handlers behind cloud-IoT are as follows: (i) *storage*, (ii) *computation*, and (iii) *communication.* Other drivers and handlers have their implications overall. These drivers and handlers are *interoperability*, *reliability*, *scalability*, *flexibility*, *availability*, *security*, *efficiency*, *data collection*, *data processing*, *reduced costs by users and providers,* and many more. This integration of cloud and IoT (cloud-IoT) has hence given birth to new paradigms to work on and to overcome the individual limitations. These new paradigms are listed in Table 8.3 for better understanding.

As we are aware that the number of connected devices is increasing day by day at an exponential rate, the data generated from them is increasing as well. This makes it almost impossible for the generated data to be stored temporarily and locally. A

Table 8.2 Complimentary characteristics of cloud computing and IoT

S. No.	Characteristics	Cloud computing	IoT
1	Displacement	Centralized	Pervasive
2	Reachability	Ubiquitous	Limited
3	Components	Virtual Resources	Real-world things
4	Computational capabilities	Virtually unlimited	Limited
5	Storage	Virtually unlimited	Limited or none
6	Role of Internet	Used for delivering service	Point of convergence
7	Big data	For management	Source

Table 8.3 cloud-IoT paradigms

S. No.	Paradigm	Description
1	Data as a Service (DaaS)	Delivering pervasive access to all kind of data
2	Database as a Service (DBaaS)	Supporting pervasive database management
3	Ethernet as a Service (EaaS)	Offering global connectivity to isolated and remote devices
4	Identity and Policy Management as a Service (IPMaaS)	Supporting abundant access to policy and identity management services
5	Sensing as a Service (SaaS)	Delivering global access to data collected by sensor
6	Sensing and Actuation as a Service (SAaaS)	Facilitating automated control actions executed in the Cloud
7	Sensor Event as a Server (SEaaS)	Forwarding message services produced by sensor actions
8	SENaaS (Sensor as a Service)	Facilitating global administration of isolated and remote sensors
9	Things as a Service (TaaS)	Accumulating and extracting diverse resources according to customized semantics
10	Video Surveillance as a Service (VSaaS)	Delivering global access to verified video and executing complex analysis in the cloud framework

solution to this problem can be a storage space leased for a dedicated amount of time so that proper analyses can be done on this data, and it gets utilized in a better way. It is a requirement for the data to be analysed and processed efficiently so that it can be converted into information and then into knowledge and can finally make the user aware about the context. Since this knowledge requires deep processing, it is not possible at IoT end only, because the devices are low in cost, are low in energy, and are light weight. This deep processing and further computation and storage can be achieved using cloud computing, and this can be done in a leased manner. As discussed above, this integration of cloud computing and IoT is termed as cloud-IoT or COT. In this integration, IoT provides efficient and sophisticated methods of communication in a distributed manner with the web, through ubiquitous devices and networks. Cloud computing, in contrast, provides scalable network access as per the requests and demands. The cloud-IoT communication is depicted in Fig. 8.10 which makes it easier for the readers to understand how the communication takes place in this integrated paradigm.

As shown in Fig. 8.10, various IoTs generate a large amount of data, where things or devices of similar nature are grouped together in a set IoT, which are passed through other layers and the data is communicated through a dedicated communication channel. The communicated data reaches the cloud layer, where it is stored,

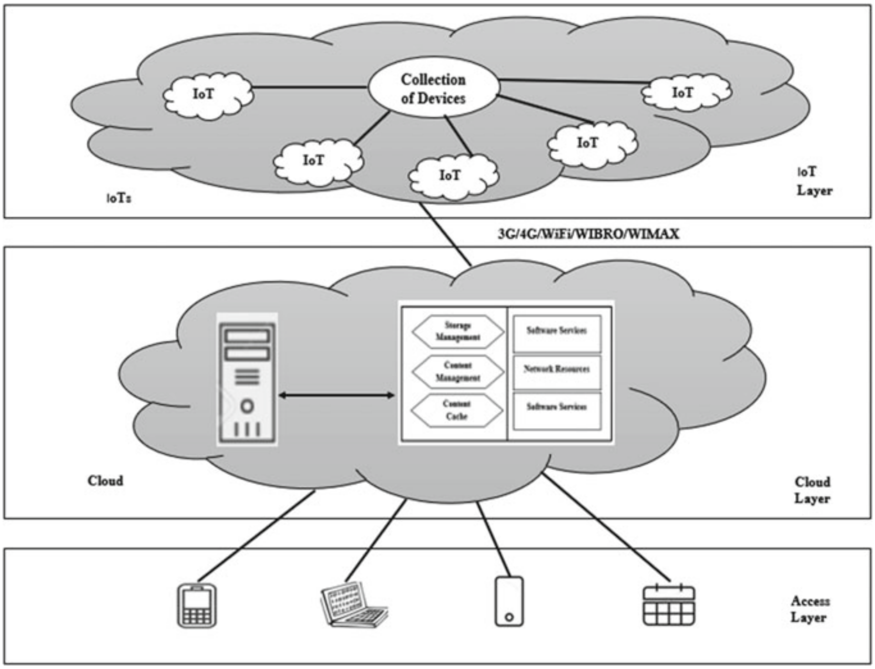


Fig. 8.10 cloud-IoT communication paradigm

analysed, processed, and managed according to the requirements of the service application. Once a service application is established, it is made available to the end-user, which resides at the access layer, at the other side of the cloud. There are several challenges faced by cloud-IoT, which are mentioned as follows: (i) *energy efficiency*: with the presence of a large number of devices and sensors, it is evident that a lot of data would be generated and hence a lot of communication and processing would take place, which in turn would consume a large amount of power. It is not possible for a temporary source of power like batteries to manage such complex communication set-up. Hence instead of temporary power generation, permanent power supply (such as solar energy) and efficient energy management is the solution to this challenge. Fog computing can also be seen as another solution to this challenge, using a localized cloud for offloading purpose; (ii) *identity management*: over the Internet, each communicating device or node has its own identification number, and with a large number of devices present, providing unique identification number to each device is quite a task. IPv6 addresses are considered to be enough to provide this kind of identification addresses; (iii) *service discovery*: as any device can be a part of IoT at any time and exit IoT at any moment, it is the responsibility of the cloud manager, also termed as cloud broker, to identify and discover new services for the users. And this responsibility keeps on staggering as complex the IoT network becomes. A more promising identification mechanism employment is needed for this type of challenge; (iv) *location of data storage*: location is also a critical point when it comes to real time, jitter prone services. Virtual storage server allocation is a solution; (v) *communication of unnecessary data*: during the entire communication and processing process, there may be some point when it is no longer necessary to sync and upload the data to the cloud. Identifying such devices whose connection is no longer valid and hence ignoring the data generated by them is also a key factor in maintaining the overall efficiency of the network. The unwanted data can be stored on a local storage location and can be linked with the network whenever required; (vi) *protocol support*: different things or devices require different protocols to connect to the network and these protocols need to coexist too. The solution to this challenge depends upon the gateway as well as the sensors. Protocols are discussed in brief in the upcoming section; (vii) *resource allocation*: the task of resource allocation is one of the most critical challenges faced by cloud-IoT. This environment deals with large number of connected devices falling into various categories, and any device can request for any resource at any point of time. The proper mapping of resource to the device must be managed, and this mapping must depend on the type, sensor, and purpose. Resource allocation algorithms must be implemented at middleware for proper allocation of resources to the devices; (viii) *IPv6 deployment*: as discussed above, IPv6 is used for identification of connected devices hence its proper, standardized, and efficient deployment is a must for which tunnelling is used; (ix) *quality of service provisioning*: such a huge amount of data bring along unpredictability and hence quality of service becomes an issue and dynamic prioritization is required; and (x) *security and privacy*: it is one of the major issue which is being faced. It is discussed in detail in upcoming sections.

8.2.2 IoT Networks Used in Fog Computing

This section is dedicated to the discussion of IoT network used in fog computing, and this hybrid system consists of fog computing which is distributed in nature along with the software-defined networking (SDN) and blockchain hypothesis and its aim is to support IoT networks and applications. The basic architecture of this fog-IoT system is represented in Fig. 8.9 and is discussed in brief in Sect. 8.1. This integrated system architecture consists of three layers: (i) *device layer*: this layer can also be termed as sensor layer or object layer (Byers 2017). This layer is a set of all IoT and sensor device present in the respective environment. As we are aware, these devices are smart devices and are connected over the Internet and are used to collect and measure the data being generated. This layer is responsible for transferring the data to the other layers of IoT network. Also, it is important to manage to the devices in an efficient manner as these devices are heterogeneous in nature; they are battery operated and have different computing, storage and processing capacities and have varied energy resources; (ii) *fog layer*: fog layer is the intermediatory layer which is responsible for deploying fog nodes for providing a medium for the data to move forward in the IoT network and enable other fog computing services (data analysis, data classification, data monitoring, etc.) to IoT network. Here, the fog nodes are deployed at the edge of the network and each node servers a set of IoT devices associated with the application. Finally, the results are forwarded the next top layer of the network, the cloud layer for further processing and acknowledgement is sent to the devices as well that the communication to the cloud layer has been established. This layer reduces the data traffic at the network as it provides an offloading path for data to move forward, also it provides end-to-end latency capability as all the computation is being done right near the devices right at the edge. Fog layer is also responsible for enhancing the network flexibility; (iii) *cloud layer*: cloud layer is the topmost layer of this system which is represented by a remote cloud unit. This layer is responsible for supporting different IoT protocols and services required by the devices and the applications. This layer provides a medium to service providers to connect with the IoT cloud and network, and to the user with the capabilities to monitor and control the resources and applications as well.

This system employs two main communication mediums to support the system and to keep control and management of the entire network. These communication mediums are as follows: (i) *SDN Technology*: The basic idea of SDN has been covered in Sect. 8.1 (Fig. 8.5). This fog-IoT system utilizes a centralized SDN controller responsible for controlling and managing distributed fog nodes and IoT devices. As shown in Fig. 8.5, there are three layers to this communication medium, *application layer*, *control layer*, and *infrastructure layer*. The distributed SDN controllers are connected by blockchain in order to provide security to the entire network. This SDN network manages the IoT devices and fog nodes via application programming interfaces (APIs) and (ii) *Blockchain Technology*: blockchain provides the security to the fog-IoT network against various attacks and is responsible for splitting the cloud layer into distributed clouds.

8.3 Security Issues, Threats, and Concerns

The most complex challenge while implementing IoT networks is the security and threat concerns, be it with cloud computing, fog computing. And hence the IoT networks too suffer from various security concerns which are essential to be dealt with (Muthanna et al. 2019). Since past few years, major research being conducted in these domains are concentrating on providing a secure platform to the end-users. There are many hurdles in the way of providing secure service, but future is hopeful. The security and threats can be classified into many categories, but broadly the different categories and their sub-categories are illustrated in Fig. 8.11.

A generalized three-level security architecture, as shown in Fig. 8.12 can be recognized, where each layer is independent with respect to security. The three layers are as follows: (i) *infrastructure layer*, (ii) *service middleware layer*, and (iii) *application layer*.

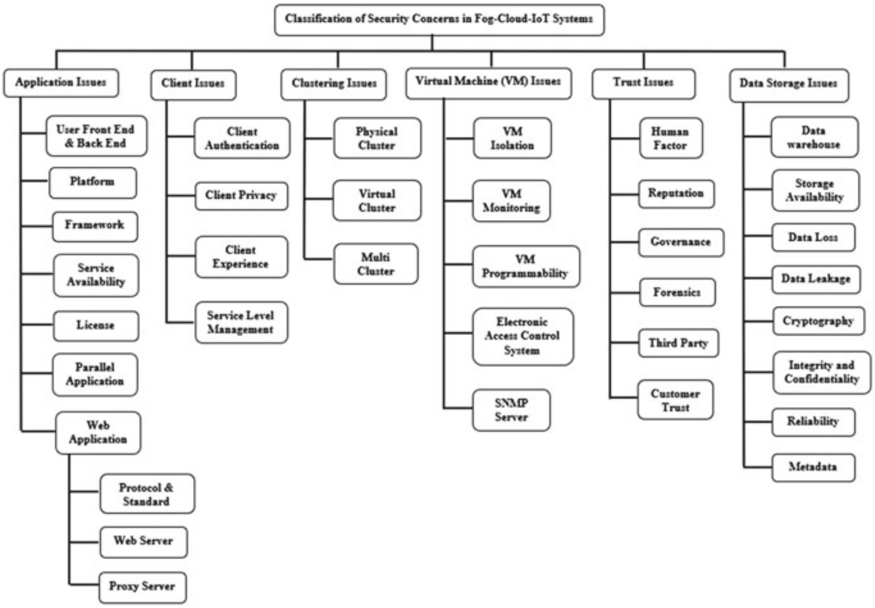


Fig. 8.11 Security categories in fog-cloud-IoT

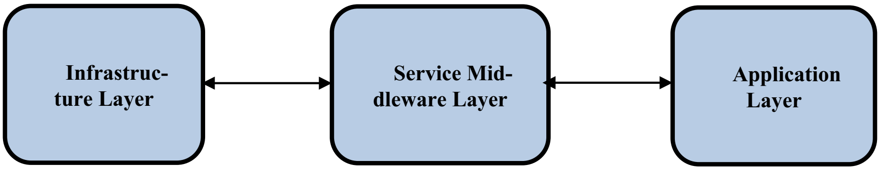


Fig. 8.12 Three-layer security architecture

Now, each layer is to be individually diagnosed for any security issues or threats. As each layer is security-independent with each other, each problem can be individually tackled without distressing about its effect on any other layer. The other layers are assumed to be working on their own, dealing with their own security issues. Figure 8.13 depicts the factors impacting each layer.

8.4 IoT Network Protocols

Since one of the components of cloud-IoT and fog-IoT is IoT, the same protocols are required in the integrated systems as are required in IoT (Dizdarević et al. 2019). This section discusses in brief about the protocol requirements in an IoT system. Figure 8.14 shows the protocol stack used in IoT system.

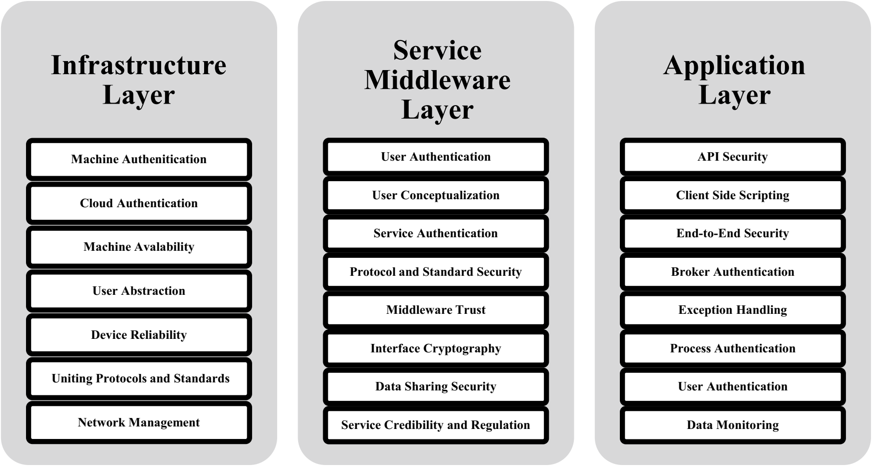
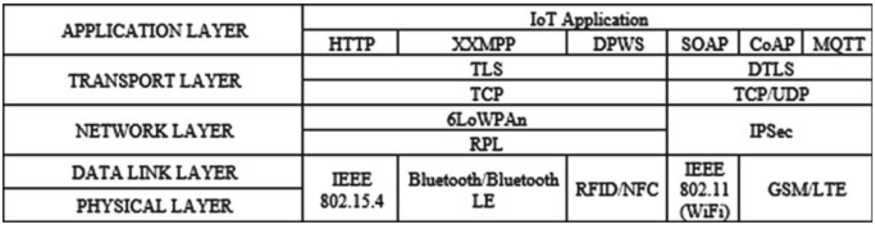


Fig. 8.13 Factor affecting three-layer security architecture



APPLICATION LAYER	IoT Application					
	HTTP	XXMPP	DPWS	SOAP	CoAP	MQTT
TRANSPORT LAYER	TLS			DTLS		
	TCP			TCP/UDP		
NETWORK LAYER	6LoWPAn			IPSec		
	RPL					
DATA LINK LAYER	IEEE 802.15.4	Bluetooth/Bluetooth LE	RFID/NFC	IEEE 802.11 (WiFi)	GSM/LTE	
PHYSICAL LAYER						

Fig. 8.14 IoT protocol stack

The application layer protocols, their main features, and comparison are depicted in Table 8.4 (Heđi et al. 2017). And the protocols used in fog-cloud-IoT environment are shown in Fig. 8.15.

8.5 Case Studies

Case Study 1: Smart City Travel Service Composition (Chen et al. 2018a)
Chen et al. (2018a) have proposed a trust-based service management protocol which they have termed as IoTHiTrust for a three-tier mobile cloud-IoT system. This protocol aims to permit IoT users to inform their cloud service experience to the IoT service provider. Authors have performed a detailed scalability analysis using ns-3 simulation. This analysis claims that this protocol achieves good levels of scalability and does not compromise on convergence, accuracy, and resilience against malicious attacks. The authors claim that this protocol outperforms the existing IoT trust management protocols in both centralized and distributed environment. They

Table 8.4 Application layer protocols

Protocol	Request–repeat model	Publish–subscribe model	Standard	Transport	QoS	Security
REST HTTP	√		IETF	TCP	–	TLS/SSL
MQTT		√	OASIS	TCP	3 Levels	TLS/SSL
CoAP	√	√	IETF	UDP	Limited	DTLS
AMQS	√	√	OASIS	TCP	3 Levels	TLS/SSL
DDS		√	OMG	TCP/UDP	Extensive	TLS/DTLS/DDS
XMPP	√	√	IETF	TCP		TLS/SSL
HTTP/ 2.0	√	√	IETF	TCP		TLS/SSL

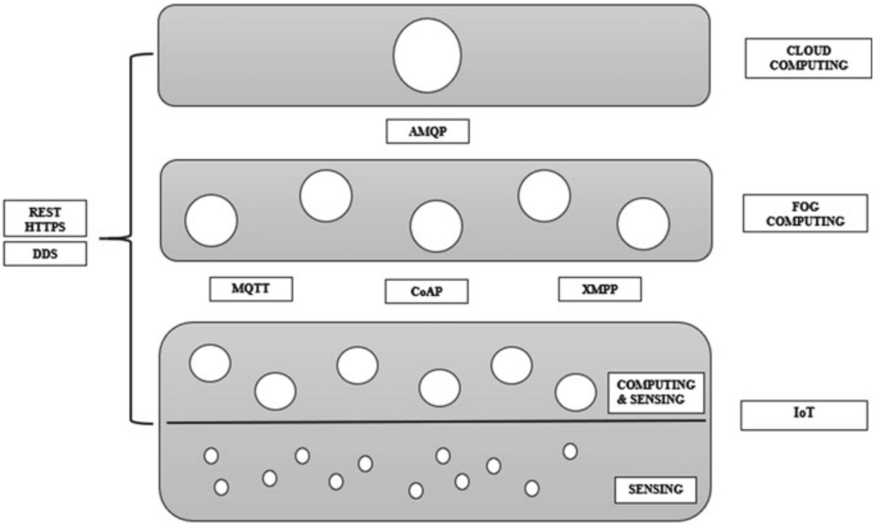


Fig. 8.15 Application protocols in fog-cloud-IoT network

have applied this protocol on two case studies to test its feasibility. The two case studies are as follows: (i) *smart city travel service composition application* and (ii) *pollution detection and response application.* The authors have applied the proposed IoTHiTrust protocol and used ns-3 simulation tool for achieving the said tasks in both case studies. The results support their claim by maximizing application performance and achieving good levels of scalability.

In this application, a traveller is exploring a city (smart city), which he has not visited yet and hence he is not sure about the quality of service to receive from the city during his visit. Since the city is a smart city, the traveller downloads a social IoT-augmented map application and registers into it. NFC-equipped smartphone can browse the tag-augmented city map and connects the traveller's smart phone to all the available IoT devices to provide information on tourist's places, food, transportation, and entertainment services. The smartphone has been instructed to make dynamic selection decisions, and hence the smartphone must: (i) *collect data or information gathered from environment either by self-observation or by recommendations*, (ii) *frame a service plan based on the results generated by step 1*, and (iii) *meet the traveller's demands by invoking the necessary services.* As discussed, authors have used ns-3 simulator to simulate the system and the three-tier system is set up as discussed. It is observed that IoTHiTrust protocol outperforms the contemporary protocols as more data is gathered.

Case Study 2: Air Pollution Detection and Response (Chen et al. 2018a)
This case study is for an application responsible for monitoring the air pollution levels of hazardous gases (CO, SO_2, NO_2, O_3, etc.) and levels of other pollutants in city. If the air pollution levels are beyond the tolerable threshold, the authorities are informed so that informed and appropriate actions can be taken in time. The area to cover depends upon the authorities, and it can range from few districts to the entire city; but the strategic plan would be to cover most polluted area of the city to observe the results in a better manner. Citizens of the city are encouraged to install the application in their smart phones to report to the authorities about the air pollution conditions in their respective areas. As discussed, authors have used ns-3 simulator to simulate the system with 2000 IoT devices which can detect and reporting the air pollutant levels to the cloud unit. A defective and malicious IoT node will always report CO levels above the threshold level and will perform ballot stuffing and badmouthing attacks to confuse the authorities. The analysis is done based upon two performance metrics: (i) *ground truth vs average CO reading* and (ii) *accuracy of trustworthy IoT nodes.* It is observed that IoTHiTrust protocol outperforms the contemporary protocols.

Case Study 3: Nested Game-Based Computation Offloading Scheme for Mobile Cloud IoT Systems (Kim 2015)
In Kim (2015), the author has proposed a novel nested game model with the aim of designing an effective mobile cloud-IoT computation algorithm. The steps are as follows: (i) *all mobile devices identify the percentage of remote offloading computation based on the tactics of rubinstein game*, (ii) *the cloud system dynamically assigns a computation resource for requested offloading computation*, and (iii) *the proposed algorithm then provides an optimum solution for the computation in mobile cloud IoT system based on the nested game principle in distributed environments.*

Case Study 4: Intelligent Transportation Systems (ITS) (Munir et al. 2017)
Munir et al. (2017) have discussed that the future of ITS performances is the integrated fog-cloud-IoT systems. As compared to a cloud ITS system, this integrated system has many advantages which are discussed here in brief: (i) all the participating ITS agents are provided Wi-Fi connectivity by the distributed fog nodes of this integrated network, (ii) with the inclusion of fog computing, the fog nodes can act as intermediate hops in communication process, (iii) data size can be effectively

reduced by performing data filtering and analysis on the collected data using fog nodes, and (iv) latency of data communication process can be drastically reduced when the data processing is done using fog nodes.

Case Study 5: Comprehensive Framework for Student Stress Monitoring (Verma and Sood 2019)
Verma and Sood (2019) have proposed a novel student-centric stress monitoring framework with the aim of predicting the stress index of students based on a particular perspective. They have used Bayesian Belief Network (BBN) for classifying the stress level and putting them in classes of normal or abnormal. The physiological parameters and readings are gathered from the medical smart devices and sensors using the fog nodes at the fog layer. The abnormal class data are further analysed for different stress related characteristics at the cloud layer. Authors have also implemented a two-level temporal dynamic Bayesian network (TDBN) model for computing the student stress index. This model operates based on analysing four different parameters: (i) *evidence*, (ii) *workload*, (iii) *health behaviours*, and (iv) *context*. Using the TDBN model, the student's stress index is generated and then actions, and decisions are taken using an alert generation method, and an alert is forwarded to the caretaker of the student (parent, guardian, etc.)

Case Study 6: Prototype of a Smart Building Application (Dutta et al. 2017)
Dutta et al. (2017) propose a prototype of a smart building and based on which they claim to have a smart city in the future. Author's aim is to improve include better quality of service, working facilities, and standard of living in home and in offices making the entire system efficient, automatic, and under the control of the user via their smart phone. They have used the integrated fog-cloud-IoT system for their prototype using open-source hardware and software. User can either be at the building or a remote site. The user at the building can control the devices through smart phone via Bluetooth, while the user at a remote site will be required to have a Wi-Fi Internet connection. The server is maintained at the cloud to manage the status of the devices and the data. Authors have suggested to include a certain number and type of devices and sensors for the prototype.

Case Study 7: Prototypes of Autism and COVID-19 Monitoring Systems (Kallel et al. 2021)
In Kallel et al. (2021), the authors have proposed a business process model and notation model to enable IoT aware business process modelling. This proposed extension is workable for both the heterogeneous IoT and non-IoT devices. Secondly, along with this extension, the authors have also proposed a novel fog-cloud-IoT-based architecture which aims to support the distributed interlayer as well as the intralayer communication of the IoT data in the system, to enable techniques to ensure data integrity within the environment, and to deploy business processing model into the fog and cloud resources. Finally, the authors have proposed the extensions for smart autistic child and COVID-19 disease monitoring systems. The data is generated for IoT devices; the behaviour of the autistic child is sent to the guardian so that

correct timely intervention can be taken. As for COVID-19 disease, the authors have proposed a system which allows the patients to be supervised in real time so that others are not contaminated with the virus. Patients' movement, their ID number, most contaminated areas of the city, and notifications and alerts to the patients, their guardians, and nearest healthcare centre are to be managed by the proposed system.

8.6 Conclusion

World is evidently witnessing a rapid increase in the use of IoT devices. Hence, the need of increase in IoT services, quality of service and management, system efficiency, and customer's satisfaction have become crucial. It is apparent that the future lies in the hybrid systems of fog-cloud-IoT technologies. Though still in infancy, the concept is picking up and is the important topic of research among the researchers. The study on the architectures and protocols is being carried on extensively and the work on the prototypes of various real-time applications is being researched. This chapter discusses the challenges faced by cloud architecture, and an integrated system of cloud-IoT or fog-IoT or fog-cloud-IoT provides potential solutions to many challenges.

References

Aazam M, Huh EN, St-Hilaire M, Lung CH, Lambadaris I (2016) Cloud of things: integration of IoT with cloud computing. In: Robots and sensor clouds. Springer, Cham, pp 77–94

Ashton K (2009) That 'internet of things' thing. RFID J 22(7):97–114

Atlam HF, Alenezi A, Alharthi A, Walters RJ, Wills GB (2017) Integration of cloud computing with internet of things: challenges and open issues. In: 2017 IEEE international conference on Internet of Things (iThings) and IEEE Green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). IEEE, pp 670–675

Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp 13–16

Botta A, De Donato W, Persico V, Pescapé A (2016) Integration of cloud computing and internet of things: a survey. Futur Gener Comput Syst 56:684–700

Byers CC (2017) Architectural imperatives for fog computing: use cases, requirements, and architectural techniques for fog-enabled iot networks. IEEE Commun Mag 55(8):14–20

Chen R, Guo J, Wang DC, Tsai JJ, Al-Hamadi H, You I (2018a) Trust-based service management for mobile cloud IoT systems. IEEE Trans Netw Serv Manage 16(1):246–263

Dizdarević J, Carpio F, Jukan A, Masip-Bruin X (2019) A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Comput Surv (CSUR) 51(6):1–29

Dutta J, Roy S (2017) IoT-fog-cloud based architecture for smart city: prototype of a smart building. In: 2017 7th international conference on cloud computing, data science & engineering-confluence. IEEE, pp 237–242

Gonzalez C, Flauzac O, Nolot F, Jara A (2016) A novel distributed SDN-secured architecture for the IoT. In: 2016 International conference on distributed computing in sensor systems (DCOSS). IEEE, pp 244–249

Heđi I, Špeh I, Šarabok A (2017) IoT network protocols comparison for the purpose of IoT constrained networks. In: 2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO). IEEE, pp 501–505

Kallel A, Rekik M, Khemakhem M (2021) IoT-fog-cloud based architecture for smart systems: prototypes of autism and COVID-19 monitoring systems. Softw: Pract Exp 51(1):91–116

Kim S (2015) Nested game-based computation offloading scheme for mobile cloud IoT systems. EURASIP J Wirel Commun Netw 2015(1):1–11

Mei G, Xu N, Qin J, Wang B, Qi P (2019) A survey of Internet of Things (IoT) for geohazard prevention: applications, technologies, and challenges. IEEE Internet Things J 7(5):4371–4386

Munir A, Kansakar P, Khan SU (2017) IFCIoT: Integrated Fog Cloud IoT: a novel architectural paradigm for the future Internet of Things. IEEE Consumer Electron Mag 6(3):74–82

Muthanna A, Ateya A, Khakimov A, Gudkova I, Abuarqoub A, Samouylov K, Koucheryavy A (2019) Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. J Sensor Actuator Netw 8(1):15

Olivier F, Carlos G, Florent N (2015) New security architecture for IoT network. Procedia Comput Sci 52:1028–1033

Ray PP (2016) A survey on internet of things architectures. J King Saud Univ Comput Inf Sci

Saharan KP, Kumar A (2015) Fog in comparison to cloud: a survey. Int J Comput Appl 122(3)

Verma P, Sood SK (2019) A comprehensive framework for student stress monitoring in fog-cloud IoT environment: m-health perspective. Med Biol Eng Compu 57(1):231–244

Wang L, Von Laszewski G, Younge A, He X, Kunze M, Tao J, Fu C (2010) Cloud computing: a perspective study. N Gener Comput 28(2):137–146

Xia F, Yang LT, Wang L, Vinel A (2012) Internet of things. Int J Commun Syst 25(9):1101

Yi S, Li C, Li Q (2015) A survey of fog computing: concepts, applications, and issues. In: Proceedings of the 2015 workshop on mobile big data, pp 37–42

Yun M, Yuxin B (2010) Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. In: 2010 International conference on advances in energy engineering. IEEE, pp 69–72

Chapter 9
Internet of Vehicles: Features, Architecture, Privacy, and Security Issues

Sushma Malik and Anamika Rana

9.1 Introduction

Nowadays, the Internet of things (IoT) technology has become the favorite technology for academics, researchers, and also for entrepreneurs because of its connecting of things characteristics. IoT seamlessly links heterogeneous devices, objects, and things to develop the physical network of things. The data acquired by IoT network devices are obtained through a sensing process, after which the data are used to communicate the devices and are controlled and maintained automatically without the need for human intervention. IoT technology becomes a domain field through the implementation of smart homes, smart cities, and also making intelligent things. IoT technology can be implemented on any device, any business, any place, and any time that is connected to the Internet or may be controlled by the Internet (Krasniqi and Hajrizi 2016). Application range of IoT from wearable devices to products used by consumers for automation, healthcare, smart farming to industrial applications, smart parking to the smart city, and now, it plays an important role in the connectivity of vehicles. Mobility is the backbone of people who live in urban areas and also acts as the vital economic factor in the development of the world (Khayyam et al. 2020). Dramatic changes are brought in the vehicles by hurried urbanization and development of megacities. Innovative resolutions like autonomy, electrification, and connectivity between vehicles are implemented. Now the question comes to mind: how do we connect the vehicles? Yes, it is possible with the implementation of technology, which can improve the quality of life of human beings. With the help of technology, development and implementation of automation in vehicles will provide

S. Malik (✉)
Institution of Innovation in Technology & Management, Janakpuri, New Delhi, India
e-mail: sushmamalikiitm@gmail.com

A. Rana
Maharaja Surajmal Institute, Janakpuri, New Delhi, India

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_9

better road safety and minimize the congestion in urban areas. Therefore, the development of intelligent transport systems (ITS) concept has been proposed with the motive of improving traffic safety and connectivity with the help of IoT technology (Lee et al. 2016). IoT is a new technology that pervades the number of ways to connect physical world with the digital world. Smart things of the world are connected and enable them to communicate with each other by this technology. IoT technology changes the planet into creative and imaginative by permitting small things and human beings to connect for communication. With the emerging technology like IoT, communication methods become more informative, processing of data become intelligent, and devices become more creative which help to communicate with each other at "anytime, anywhere, anyway, anything." When smart objects like vehicles are connected over the Internet, at that time, IoT becomes the Internet of vehicles (IoV) (Joy and Gerla 2017). IoV technology used three types of networks like one is the network in between vehicles, the second one is the network within the vehicle, and the last one is the network of vehicles with the mobile (Meeting 2014). So it can be said that IoV is an extended application of IoT to make an intelligent transportation system. It captures the data through the sensors and provides the processing platform for the ITS. In IoV, a vehicle will capture data through sensors from the environment, from the vehicle's driver and other vehicles and after processing the captured data using for safe navigation, pollution control and in also manage the traffic on the road (Sharma and Kaushik 2020). Like IoT technology, human control is removed on devices, and vehicles become autonomous vehicles. Smooth traffic flow can be maintained on roads by autonomous vehicles automatically, visibly, and efficiently. According to introspective persons, the performance of autonomous vehicles will give better results as compared to human drivers, effectively handle traffic, and also improve driver and passenger safety. Vehicles with IoV technology have some features like storage of data capability, smartness with learning, and communication to foresee the intents of the user. IoV innovation is gainful in handling different traffic and driving issues and gives the safety of travelers and facilitates the whole driving experience (Tangade 2013).

IoV technology network acts as the heterogeneous vehicular network in which communication can occur between vehicles and with vehicles, roadside things, user personal devices, sensors, and many more objects of the world. Wireless technologies that are used by the IoV platform for communication are mobile networks (4G/LTE and satellite) and small ranges like Zigbee, Bluetooth, and Wi-Fi (Guo et al. 2007, Contreras-castillo et al. 1839). Vehicles produced lots of information daily, and now, vehicles can store the data and after analyze share the information to implement the safety and also save the travel time by the implementation of IoV. Advanced driver assistance system (ADAS) in IoV plays a vital role to overcome traffic issues and also improve the driver's experience. Empowered sensors on the road as well as on vehicles can detect the condition of traffic like vehicle stream, its speed, and car crashes. Collected data from sensors are shared between vehicles or backend servers to understand the condition of traffic and on that basis provide information to vehicles (Bonomi et al. 2013).

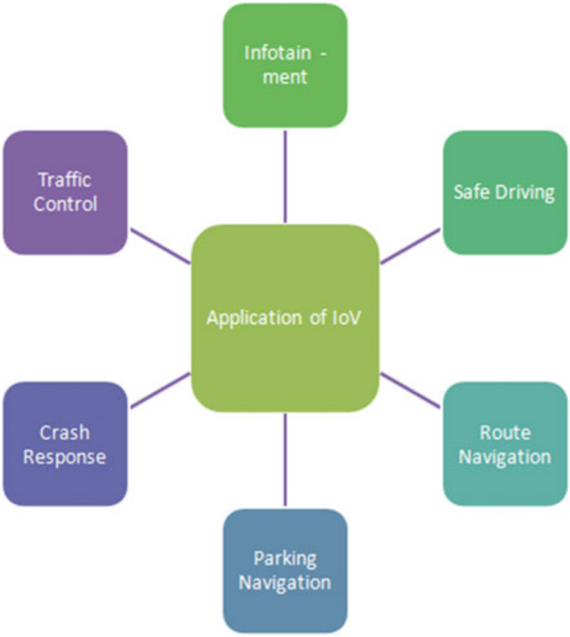
For the change of normal vehicles to savvy vehicles, more and more endeavors are carried out on research and development. Almost all main manufacturers like Toyota, Ford, GM, BMW, Volvo, etc., all have started their intelligent vehicles projects, and also major IT companies like Google, Apple, and Huawei are working on intelligent vehicles systems. In IoV technology, vehicles are playing the dual role as they work as a client that consumes the services from the Internet and at the same time perform distributed computing in between peers.

9.2 Applications of Internet of Vehicles

IoV technology has diverse solicitations. On the basis of functionalities, IoV applications (Sharma and Kaushik 2020) are shown in Fig. 9.1.

1. **Safe Driving**: This application mainly refers to cooperative collision avoidance systems (CCAS) (Sharma and Kaushik 2020) which extended the collisions avoidance system (CAS). It uses the sensors to sense the forthcoming collision and warn the driver and sharing information among the nearest vehicles. It sends the status messages and emergence messages that are triggered by emergency conditions like a traffic jam, accident, and condition of the road.
2. **Route Navigation**: In this, GPS is used to find the route, and it also shares the user about the real-time traffic information and consumption of fuel. The author

Fig. 9.1 Applications of Internet of Vehicles (IoV)



of Collins and Muntean (2008) offered a route selection algorithm that helps to solve congestion of traffic by improving the utility of roads.

3. **Traffic Control**: Control of traffic at the intersection has a major concern for the IoV technology. The core worried points are that how to plan traffic signals efficiently based on the traffic volume to minimize the waiting time. A controller node is put at the intersection regions which help to gather the line length of vehicles and figure the cycle time of the signal by Webster formula (Gradinescu et al. 2007), and priority of vehicles is considered in Wunderlich et al. (2008).
4. **Crash Response**: In IoV, all the vehicles are associated and naturally send the real-time information about the accident with area to the emergency handling team, and the team can provide the immediate service to the user and also save the life.
5. **Parking Navigation**: In urban areas, finding the parking space is a major problem. But with IoV, this problem can be solved by implementing a smart parking system. In (Verroios et al. 2011), introduced a new methodology to compute the parking space that a vehicle to move.
6. **Infotainment**: Vehicles act as the smarter with the implementation of IoV. Vehicles can access the Internet services, streaming videos, and share the information with the dashboard. Communication of vehicles with the Internet is a challenging task and to sort out that difficulty (Ksentini et al. 2010) by introducing a framework to ensure to forward data through the Internet on highways.

9.3 Interaction Model in IoV

The main motive of IoV technology is consistent integration of all components like vehicles, sensors, specialized gadgets, side of the road framework, client and individual gadgets to improve the security, and solace level of the people. Figure 9.2 shows the key parts of the IoV technology that communicates with others, like (Kaiwartya et al. 2016, Contreras-castillo et al. 1839):

- **Vehicle (V)**: In IoV system, vehicles are included the adjacent vehicles that establish the communication link for the conversation.
- **Person (P)**: Person includes the users that request or access the data and services in the IoV domain.
- **Personal Device (PD)**: Personal devices are those devices that belong to the user, and these devices using or provide the services in IoV environment.
- **Network Infrastructure (I)**: It includes all the network gadgets used to send the information.
- **Sensing Devices (S)**: Data generators and data receivers are the sensors and actuators that collect information about the parameters of vehicles like the temperature of the vehicle, utilization of fuel, and tire pressure. They collect the user’s health condition like heart rate, blood pressure, and oxygen level in the blood. These sensors are also collect environmental data like pollution and noise level, weather conditions, etc.

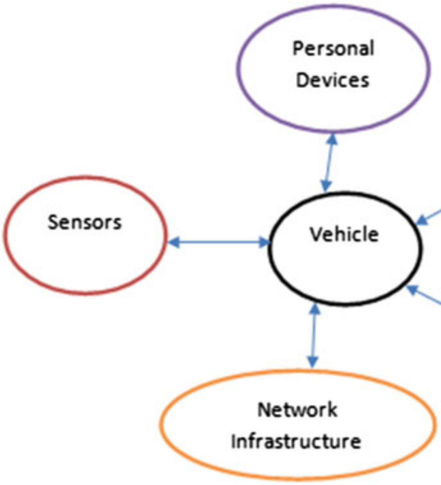


Fig. 9.2 Interaction model in Internet of vehicles (IoV)

- **Roadside Devices (R)**: Roadside devices are the infrastructure of transportation systems like traffic lights, radars, and information screens.

9.4 Literature Review

S. No.	References	Description
1	Krasniqi and Hajrizi (2016)	Examine the market and technology trends toward autonomous vehicles, the importance of IoT technology in the vehicles industries. 5G technology is used for the communication between vehicles
2	Sadiku et al. (2018), Wu et al. (2016)	IoV technology has become the essential part for the user and design intelligent transportation system that without traffic lights and other problems. It provides convenient, comfortable, and safe transport services
3	Jameel et al. (2019)	Proposed a new paradigm called the Internet of autonomous vehicles (IoAV) to remove the drawbacks linked with autonomous vehicles. Also highlights the key features, application for IoAV which provide a performance improvement

(continued)

(continued)

S. No.	References	Description
4	Khayyam et al. (2020)	The architecture of new AI-based autonomous vehicles is proposed by using edge computing. The integration of AI and IoT technologies will provide highly performed embedded systems
5	Lee et al. (2016)	IoV implemented vehicles have communications, storage, and learning capability to fulfill the user's intentions. Introduced the vehicular fog that equal to the Internet cloud for transportations
6	Joy et al. (2018)	Presented the architecture of heterogeneous communication technologies that make possible to communicate V2V and V2I to provide the support in IoV. Vehicles generate a piece of huge information stored on the cloud which provides various services like routes based on traffic after analyzing data on the cloud. Also presented the approaches to provide the security and privacy to vehicular clouds which provide more safer and comfortable vehicular transportation
7	Ahangar et al. (2021), Mokhtar and Azab (2015)	In IoV technology, vehicles are collect and generate the large amount of data through enabled sensors, and after analyzing data for the decision, the ad hoc network topology enables the autonomous vehicles to communicate with each other and with the network with the implementation of rad safety and flow of traffic
8	Khayyam et al. (2020)	IoV is an incorporated framework that joins the client inside and around vehicles. It gains popularity and esteem examination because of the fast advancement of communication and computation innovative technologies like big data, grid computing, and AI
9	Lee et al. (2016), Joy and Gerla (2017)	Present the essential premises for the advancement of IoV with the integration of big data analytics of road networks. Gave more concern to the fog computing layer which is used to design the agenda for real-time collection and data processing

(continued)

(continued)

S. No.	References	Description
10	Meeting (2014)	The number of devices like sensors, user's devices need to communicate with each other, but they facing challenges like incompatibility, response time for the connection of the Internet, storage capability, and restricted processing during design. Proposed the structure that provides seamless integration for between gadget communication
11	Sharma and Kaushik (2020), Qu et al. (2015)	Vehicular ad hoc network (VANET) technologies are using mobile-based routing protocols for sharing of information to implement the smart transportation network. Confidentiality and security are the key concern during the development of smart vehicles
12	Tangade (2013), Jain (2014)	Introduce the five characteristics of IoV system like dynamic topological structure, distribution of nodes in a non-uniform manner, granularity diversity, huge-scale network, and limitation of mobile
13	Contreras-castillo et al. (1839)	Data can be collected into the open database source and shared among the number of collaborators in IoV. Introduced the Haystack privacy which provides strength in privacy as a large number of owners participate yet maintains accuracy
14	Bonomi et al. (2013), Zheng et al. (2015)	Highlight the remunerations of IoV technology and also present the recently introduced protocols for the communication which help the grouping of vehicles in the IoV technology
15	Sharma and Kaushik (2019)	Introduced the social Internet of things (SIoT) that establishes the social relationship between the objects and creating the social network in which instead of human beings participates are the intelligent objects
16	Collins and Muntean (2008)	Suggested a mobile crowd sensing approach to provide dynamic route choice for the drivers and stay away from the congestion
17	Gradinescu et al. (2007)	Introduced the edge information system (EIS) for IoV technology by implementing edge computing, edge caching, and edge AI. The main point of EIS is to play the main component of the information infrastructure that supports IoV

(continued)

(continued)

S. No.	References	Description
18	Wunderlich et al. (2008), Chu and Huang (2012)	Offered a new approach to satisfy the requirements of self-governing driving errands with the rationale to raise the insight, processing, and transportation execution in the cognitive Internet of vehicles
19	Verroios et al. (2011)	Examined that how blockchain technology is implemented in the vehicle networking with the main effort on the distributed and protected storage of big data
20	Ksentini et al. (2010), Hossain et al. (2010), Dak et al. (2012)	IoV is the active research field that is the combination of VANETS and IoT technologies. Between vehicular correspondence, intra vehicular correspondence, and vehicular mobile Internet are the three primary communication components of IoV. 5G network has good bandwidth to enhance the communication in between the connected devices
21	Sadiku et al. (2018), Wu et al. (2016)	IoV technology gives a worldwide scope and facilities which gives brainy vehicles networks with the capability of communication in vehicles by Internet
22	Jameel et al. (2019), Joy et al. (2018)	Collaborative networking has heterogeneous vehicular network in IoV and using the different types of the heterogeneous network like WAVE, Wi-Fi, 4G/LTE, and satellite. It enhances the flexibility of architecture in IoV
23	Ahangar et al. (2021), Qian and Moayeri (2008)	Data cannot be altered during the transmission process for efficient and secure communication. But in IoV technology, vehicles have a dynamic network and high mobility which make difficult to ensure security of data
24	Nahri et al. (2018)	Mobility adaptive clustering information reduction (IR) and the VAC multihop forwarding method are integrated to provide the efficient overlay forwarding solution to communicate vehicular traffic. The solution is to design the lightweight, message-driven, and distributed

The characteristics of vehicles which are implemented with IoT technology have a number of characteristics that differ these IoT enabled vehicles with normal like shown in Fig. 9.3 (Golle et al. 2004, Tuyisenge et al. 2018):

- **High Mobility**: IoV must accomplish the high mobility of the vehicles and also provide the wireless communication.

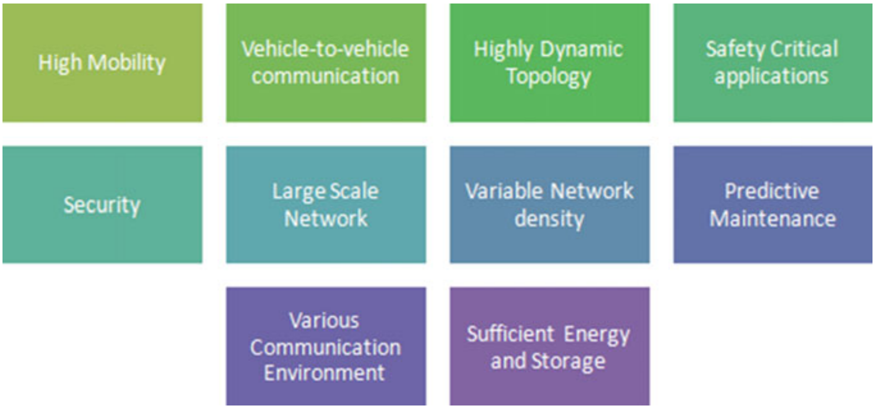

High Mobility
Vehicle-to-vehicle communication
Highly Dynamic Topology
Safety Critical applications
Security
Large Scale Network
Variable Network density
Predictive Maintenance
Various Communication Environment
Sufficient Energy and Storage

Fig. 9.3 Characteristics of vehicles in Internet of vehicles (IoV)

- **Vehicle-to-Vehicle Communication**: In IoV, short-range communication can be possible in between the connected vehicles.
- **Highly Dynamic Topology**: Vehicles may move at high velocity which influences the topology of vehicular network and much of the time adjust. This highly dynamic network topology is carefully developed for IoV.
- **Safety–Critical Applications**: Vehicles should have low latency and high reliability in the IoV domain.
- **Security**: Security is the core apprehension in the development of IoV. Because false data transmission through hackers or from malicious agents may affect the functioning of vehicles.
- **Variable Network Density**: In IoV, network density varies from high to low which depends on the traffic. In case of traffic jam, the density is high and is low in normal traffic.
- **Large-scale Network**: The network area of IoV is large in dense, urban areas like city, highways, etc.
- **Sufficient Energy and Storage**: In IoV, vehicles are acted as the nodes, and each node needs sufficient energy for computing and storage space after processing data.
- **Various Communication Environment**: Vehicles in IoV usually operated in different communication environments. Like in highways, the communication environment is simple as compare to the city because in the city number of obstacles occur like trees, buildings, etc., in the communication path.
- **Predictive Maintenance**: Sensors implemented in vehicles are monitor the functioning of vehicles like temperature, engine status, speed, and navigation. This collected information from sensors is used to update the user with preventive and predictive maintenance alerts before the issues arise.

9.5 Challenges in IoV

The main objective of employment of IoT technology in the transport domain is to integrate the number of users, vehicles, items, and numerous networks to give the best connectivity that can be easily managed, controlled, and operated. The connectivity of vehicles creates a complex system because of their dynamic nature and special kinds of requirements are desired to design this complex system. But these aspects bring the new technical challenges that face during the design and expansion of the IoV domain. Some of the challenges are highlighted in Fig. 9.4 are like:

- **Poor Network Connectivity**: Vehicles are moving from one place to another place which cause the disconnection of network frequently. Communication links act as the challenging phase in the dynamic condition.
- **Stability**: Vehicles by their nature are dynamic so stability is also the main challenge face by the vehicles in this domain. Because in some areas like hill areas, Internet facility is not available.
- **Delay Constraint**: Many IoV applications have a hard delay constraint because a minimal delay during the passage of messages among the connected devices would be crucial.
- **Big Amount of Data**: In IoV technology, connected vehicles generate the large amount of data which stored in the cloud. Insufficient storage and network delay can affect the cloud computing and also damage the system.
- **Reliability**: Applications driving-related is usually sensitive about safety because such applications have required high reliability. But in IoV implemented applications, reliability concept become crucial because of complex network architecture of applications, large network scale, and also the poor stability of the network.

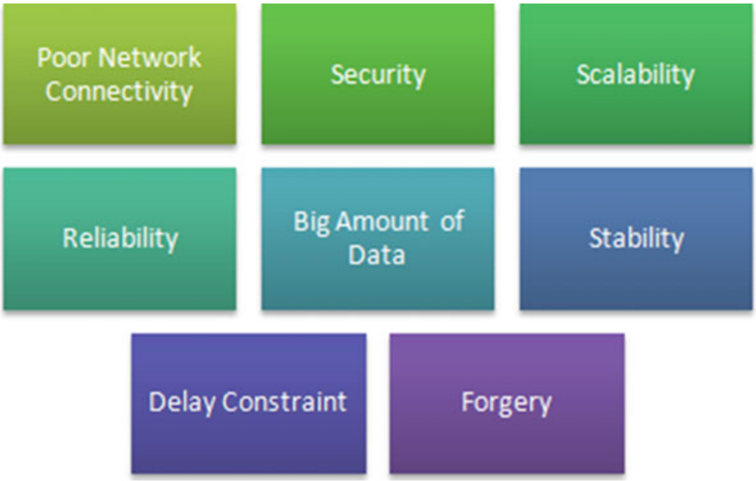


Fig. 9.4 Challenges faced in Internet of vehicles (IoV)

- **Scalability**: It is another challenge faced by the IoV domain due to the dynamic nature of the vehicles, these applications required the high scalability.
- **Security**: Security is one of the core challenge faced by IoV domain. IoV is a network that is accessed by various devices and integrates different technologies and standards through the Internet. Parts of IoV vehicles like GPS, cameras, sensors, brakes, and accelerator are remotely accessed and if the security is weak at that time successful attack can lead to control the functioning of vehicles.
- **Forgery**: The attacker can use false alarms to disrupt communication among the vehicles in the IV network. As a result, the vehicles should be able to withstand this condition.

9.6 Architecture of IoV

Currently, now, many researchers and industries are trying to design and develop a new network architecture that competently provides permission for the IoV implementation in the related business market. Four-layer architecture is proposed by Abdulkader et al. (2017) that shown in Fig. 9.5 which includes the 4 steps which involve in the IoV communication.

Five layered architecture is introduced by Sun et al. (2017) which explained by Fig. 9.6 and contain the following layers:

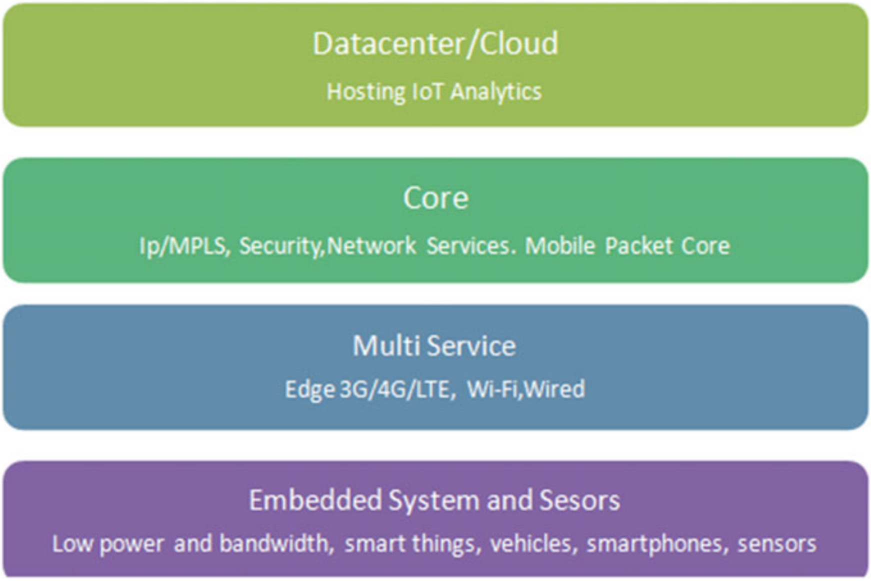
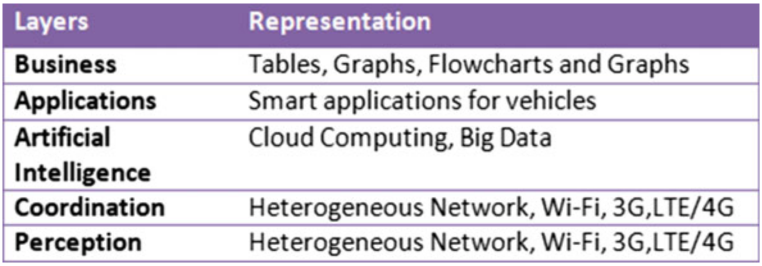

Datacenter/Cloud
Hosting IoT Analytics
Core
Ip/MPLS, Security,Network Services. Mobile Packet Core
Multi Service
Edge 3G/4G/LTE, Wi-Fi,Wired
Embedded System and Sesors
Low power and bandwidth, smart things, vehicles, smartphones, sensors

Fig. 9.5 Four-layer architecture of Internet of vehicles (IoV)



Layers	Representation
Business	Tables, Graphs, Flowcharts and Graphs
Applications	Smart applications for vehicles
Artificial Intelligence	Cloud Computing, Big Data
Coordination	Heterogeneous Network, Wi-Fi, 3G,LTE/4G
Perception	Heterogeneous Network, Wi-Fi, 3G,LTE/4G

Fig. 9.6 Five-layer architecture of Internet of vehicles (IoV)

- **Perception Layer**: This layer contains many types of sensors and actuators that are connected to vehicles, cellphones, and other devices. The core motive of this layer is gathering the data from the sensors and actuators which used in vehicles decisions. It is also responsible to transfer the information to the coordination layer in a secure way.
- **Coordination Layer**: This layer includes the network coordination modules for a heterogeneous network like WAVE, Wi-Fi, 4G/LTE, and satellite network. The accountability of this layer is to receive the data from the lower layer securely and transferred it to the upper layer which is the artificial intelligence layer. This layer's primary goal is to process the various data structures received from the heterogeneous network and combine them into a cohesive form.
- **Artificial Engineering**: AI is the third layer which is called the brain of IoV because it processes the stored data and analyzed the data which received from the lower layer and aids in the process of decision-making.
- **Application**: The fourth layer of the architecture is the applications of vehicles. It provides smart devices to the person on the idea of intelligence and analysis of data by AI layer. It also helps to transfer the end-user data to the business layer.
- **Business**: This layer is the preceding layer of the architecture which represents the operational management modules. The main obligation of this layer is to expand the business models based on the data. Different types of tools like graphs, flowcharts, and use case diagrams and comparisons charts are the major part of this layer.

Seven-layer architecture of IoV is proposed by Contreras-Castillo et al. (2017) that shown in Fig. 9.7 which allow the transparent interconnection of all components of network and data distribution in IoV atmosphere that includes the following layers:

- **User-Vehicle Interaction**: This layer basically manages the interface among the driver and vehicles and also manages the notifications.
- **Acquisition**: The main work of this layer is to accumulate the information from various sources and also convert the data in the proper arrangement.
- **Pre-processing**: This layer filters the data collected from diverse sources and is also classified based on requirements.

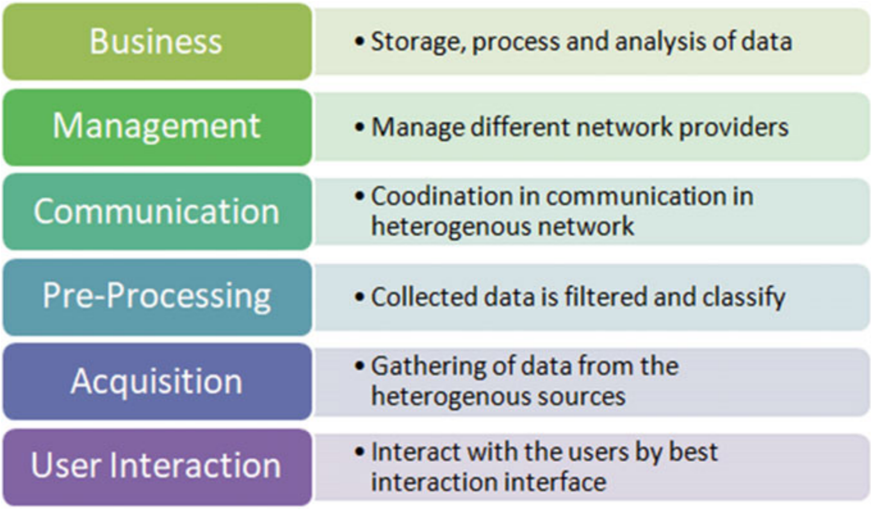

Business
• Storage, process and analysis of data
Management
• Manage different network providers
Communication
• Coodination in communication in heterogenous network
Pre-Processing
• Collected data is filtered and classify
Acquisition
• Gathering of data from the heterogenous sources
User Interaction
• Interact with the users by best interaction interface

Fig. 9.7 Seven-layer architecture of Internet of vehicles (IoV)

- **Communication**: The main motive of this layer is to coordinate the heterogeneous network and choose the best network for communication.
- **Management**: The management layer implements the measures of the network and also manages the different network services providers.
- **Business**: The main motive of this layer is to analyze the data and also set the strategies of different network providers. IoV is proposed by Contreras-Castillo et al. (2018) that shown in Fig. 9.7 which allow the transparent interconnection of all components of network and data distribution that includes the following layers:

The three-layer architecture of IoV is given by Kang et al. (2018) and shown in Fig. 9.8. It involves the following layers:

- **Perception Layer**: This layer contains the sensors of vehicles which are used by vehicles to collect the data from the environment like driving patterns, speed of vehicles, and environment conditions.
- **Network Layer**: This layer is the communication layer because it ensures connectivity with communication networks like GSM, Wi-Fi, WLAN, and Bluetooth.
- **Application Layer**: The main duty of this layer is storage of data which received from the heterogeneous sources, analyzing, and processing of data which help in the decision-making process. It includes statistical tools.

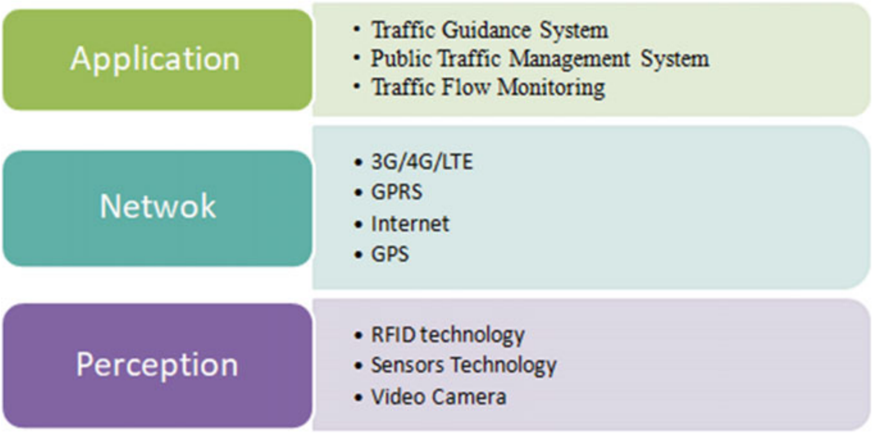


Fig. 9.8 Three-layer architecture of Internet of vehicles (IoV)

9.7 Security Aspect of IoV

In IoV technology, security is one of the main factors for the implementation of this technology. So, security is the most difficult issue in an IoV because if any vehicle is controlled by a hacker with an incorrect understanding, it will cause major traffic problems and possibly cause traffic accidents. This section will examine many facets of security, such as security requirements and issues encountered during implementation.

9.8 Requirements of Security in IoV

In IoV, security requirements are utilized to determine how safe a network is? and need to identify before the deployment of any work are shown in Fig. 9.9 and like (Sharma and Kaushik 2019):

- **Authentication**: It verifies the vehicles which involved in the communication method in IoV are authenticate otherwise this unauthenticated node can be used by the attackers for sending the message on the network (Sharma and Kaushik 2019).
- **Confidentiality**: In the communication method, data are playing a crucial role. As is the necessity to protect sensitive data so that only authorized users have access to it.
- **Availability**: The value of data is when needed otherwise the data are insignificant. So the data should be available to the genuine user when it needs (Wan et al. 2016).
- **Data Integrity**: Data integrity refers to the fact that data should not be altered, either intentionally or accidentally, while transmission via a communication

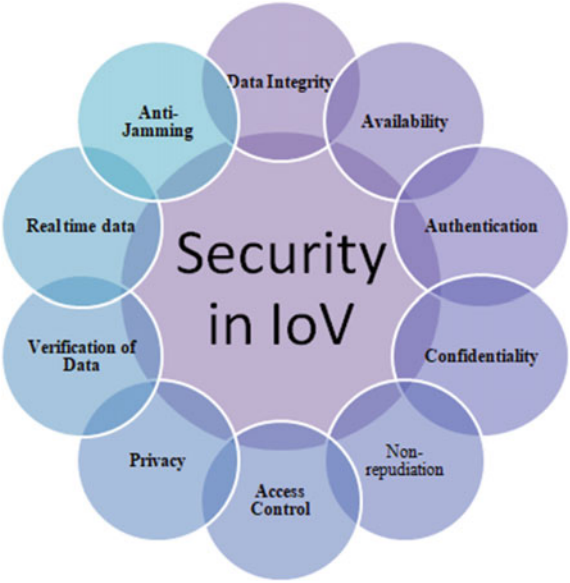
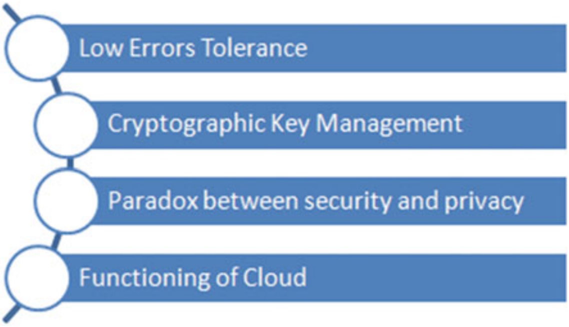


Fig. 9.9 Security concern of Internet of vehicles (IoV)

medium. To implement this, a data signature is used with a password (Zhang and Letaief 2020; Lu et al. 2019).

- **Non-repudiation**: This security mechanism is used to prevent the sender or receiver from refusing to transfer the communication (Renu and Saxena 2020).
- **Access Control**: This ensures that vehicles carry out their duties correctly.
- **Privacy**: The path used by the vehicles to move is the privacy of the user, and it cannot disclose that where the user is going and with whom because the vehicles are traced in IoV technology. That is why privacy should be implemented and cannot be accessed by an unauthorized user.
- **Verification of Data**: The regular verification of data is carried out in the IoV communication to avoid altered or fake information by malicious nodes or vehicles.
- **Real-time data**: In IoV technology, real-time applications are employed, thus the proper information should be delivered at the right moment to ensure that the time limitation in these applications is met; otherwise, providing the safety message with a delay may cause problems for the user.
- **Anti-jamming**: To stop the communication in IoV technology, malicious nodes or vehicles are act as the jammer by the DoS kind of attacks. It should ensure that no attackers are allowed to use jamming in the network (Priyan and Usha Devi 2019).

Fig. 9.10 Security challenges in Internet of vehicles (IoV)


Low Errors Tolerance
Cryptographic Key Management
Paradox between security and privacy
Functioning of Cloud

9.9 Security Challenges in IoV

Various challenges are should be considered during the implementation of IoV

- **No Tolerance of Error**: Real-time communication is hampered by poor network quality. Minor errors or delays, on the other hand, are not tolerated with IoV technology because they may result in tragedy.
- **Cryptographic Key Management**: In the IoV, the key is the most important part of the cryptographic technique that is used to encrypt and decrypt sensitive data. Key management issues should be taken seriously during the designing of security protocols (Yang et al. 2014) technology. Some security challenges are the highlight in Fig. 9.10.
- **Paradox between Security and Privacy**: More secure system will have less privacy because IoV technology could track the movement of vehicles for efficient communication and sometimes users are do not want to share their location. So balancing security and privacy are a big task (Sadio et al. 2017).
- **Functioning of Cloud**: In terms of data storage, IoV technology uses cloud services to handle huge data. Efficient encryption algorithms are implemented in both data storage and transmission in between the cloud and the user. The basic need in IoV technology is to provide the stable, secure, and private.

9.10 Future Direction of IoV

Internet of vehicles is an essential application of IoT technology in the transport domain. It involves a number of research fields like mobile computing, wireless communication, and cloud computing, and even autopilot vehicles. Still, IoV is in the initial stages, and a number of technical issues discussed above are addressed before the acceptance and deployment of IoV (Sadiku et al. 2018; Tuyisenge et al. 2018). These are some points that should be investigated further in future:

- **Efficient Information Routing and Broadcasting**: For IoV, the MAC protocol family is being developed. In the vehicular environment, routing a message at network level is an interesting topic. Till now, routing or dissemination protocols are does not appear yet.

- **Communication Based on Software-Defined Networking (SDN)**: Till now, little work has been done on software-defined vehicular networks which are not sufficient for IoV technology because of the dynamic nature of vehicles. But is still challenging for suitable link control and allocation algorithm in SDN. Due to the dynamic nature of vehicles in vehicular links are differ from wired WAN environments which create a challenge to control and allocate the resources.
- **Communication Based on Named Data Networking (NDN)**: NDN, like SDN, is another future Internet networking technology. Transportation of information on the non-predefined path of vehicles is the main motive of IoV. But NDN is not widely studied for IoV technology
- **IoV Data Processing**: Due to the increasing number of vehicles equipped with intelligent devices and the addition of roadside units, vehicular data will grow at a rapid rate daily. IoV will gain greater understanding and performance as a result of a large volume of traffic data. However, handling and processing a large amount of traffic data pose new issues in and of itself.
- **New Application**: In IoV technology, new applications are more desirable. Several new IoV-based applications are developed based on user requirements. With the help of more efficient networking, cloud computing, and big data processing techniques, these new technologies give new functionality. New applications, such as an intelligent traffic status report, real-time navigation, inter-vehicle entertainment, and so on, maybe developed in future.

9.11 Conclusion

Internet of vehicles has become the main empowering technology to get future independent driving scenarios. IoV technology is an integration of IoT technology with vehicles. This technology gains huge commercial interest and also research value because of the fast development of communication technologies like grid and edge computing, big data analysis, AI, and many more. This chapter includes the applications of IoV technology with its architecture. Also, highlight the issues in the implementation of IoV in reality after then explanation of the security aspects of IoV. Based on a survey, it analyzed that Internet technology has great potential in the current transportation system, but still, it has many issues which required to be taken into consideration. IoV plays an important role in the vehicle's different areas like safety, health, and comfort of the user with infotainment.

References

Abdulkader ZA, Abdullah A, Taufik Abdullah M, Ahmad Zukarnain Z (2017) Vehicular ad hoc networks and security issues: survey. Mod Appl Sci 11(5):30. https://doi.org/10.5539/mas.v11n5p30

Ahangar MN, Ahmed QZ, Khan FA, Hafeez M (2021) A survey of autonomous vehicles: enabling communication technologies and challenges. Sensors (switzerland) 21(3):1–33. https://doi.org/10.3390/s21030706

Bonomi F, Fellow C, President V, Others M, Architecture A, Systems C (2013) The Smart and Connected Vehicle and the Internet of Things

Chu YC, Huang NF (2012) An efficient traffic information forwarding solution for vehicle safety communications on highways. IEEE Trans Intell Transp Syst 13(2):631–643. https://doi.org/10.1109/TITS.2011.2177456

Collins K, Muntean GM (2008) Route-based vehicular traffic management for wireless access in vehicular environments. IEEE Veh Technol Conf, pp 3–7. https://doi.org/10.1109/VETECF.2008.261

Contreras-Castillo J, Zeadally S, Ibañez JAG (2017) A seven-layered model architecture for internet of vehicles. J Inf Telecommun 1(1):4–22. https://doi.org/10.1080/24751839.2017.1295601

Contreras-Castillo J, Zeadally S, Guerrero-Ibanez JA (2018) Internet of Vehicles: architecture, protocols, and security. IEEE Internet Things J 5(5):3701–3709. https://doi.org/10.1109/JIOT.2017.2690902

Contreras-castillo J, Zeadally S, Antonio J, Ibáñez G (2017) A seven-layered model architecture for Internet of Vehicles, vol 1839. https://doi.org/10.1080/24751839.2017.1295601

Dak AY, Yahya S, Kassim M (2012) A literature survey on security challenges in VANETs. Int J Comput Theory Eng 4(6):1007–1010. https://doi.org/10.7763/ijcte.2012.v4.627

Golle P, Greene D, Staddon J (2004) Detecting and correcting malicious data in VANETs, pp 29–37

Gradinescu V, Gorgorin C, Diaconescu R, Cristea V, Iftode L (2007) Adaptive traffic lights using car-to-car communication. IEEE Veh Technol Conf 1:21–25. https://doi.org/10.1109/VETECS.2007.17

Guo J, Baugh JP, Wang S (2007) A group signature based secure and privacy-preserving vehicular communication framework. In: 2007 Mobile Network Vehicle Environment MOVE, pp 103–108. https://doi.org/10.1109/MOVE.2007.4300813

Hossain E et al (2010) Vehicular telematics over heterogeneous wireless networks: a survey. Comput Commun 33(7):775–793. https://doi.org/10.1016/j.comcom.2009.12.010

Jain S (2014) Security threats in manets: a review. Int J Inf Theory 3(2):37–50. https://doi.org/10.5121/ijit.2014.3204

Jameel F, Chang Z, Huang J, Ristaniemi T (2019) Internet of autonomous vehicles: architecture, features, and socio-technological challenges. IEEE Wirel Commun 26(4):21–29. https://doi.org/10.1109/MWC.2019.1800522

Joy J, Rabsatt V, Gerla M (2018) Internet of Vehicles: enabling safe, secure, and private vehicular crowdsourcing. Internet Technol Lett 1(1):e16. https://doi.org/10.1002/itl2.16

Joy J, Gerla M (2017) Internet of vehicles and autonomous connected car—privacy and security issues. In: 2017 26th International conference on computer communication networks, ICCCN 2017. https://doi.org/10.1109/ICCCN.2017.8038391

Kaiwartya O et al (2016) Internet of Vehicles: motivation, layered architecture, network model, challenges, and future aspects. IEEE Access 4(September):5356–5373. https://doi.org/10.1109/ACCESS.2016.2603219

Kang J, Yu R, Huang X, Zhang Y (2018) Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Trans Intell Transp Syst 19(8):2627–2637. https://doi.org/10.1109/TITS.2017.2764095

Khayyam H, Javadi B, Jalili M, Jazar RN (2020) Nonlinear approaches in engineering applications

Krasniqi X, Hajrizi E (2016) Use of IoT technology to drive the automotive industry from connected to full autonomous vehicles. IFAC-PapersOnLine 49(29):269–274. https://doi.org/10.1016/j.ifacol.2016.11.078

Ksentini A, Tounsi H, Frikha M (2010) A proxy-based framework for QoS-enabled internet access in V ANETS. In: 2010 2nd International conference on communication networking, ComNet 2010. https://doi.org/10.1109/COMNET.2010.5699820

Lee EK, Gerla M, Pau G, Lee U, Lim JH (2016) Internet of Vehicles: from intelligent grid to autonomous cars and vehicular fogs. Int J Distrib Sens Netw 12(9). https://doi.org/10.1177/1550147716665500

Lu H, Liu Q, Tian D, Li Y, Kim H, Serikawa S (2019) The cognitive Internet of Vehicles for autonomous driving. IEEE Netw 33(3):65–73. https://doi.org/10.1109/MNET.2019.1800339

Meeting WG (2014) White paper of Internet of Vehicles (IoV). 50th Telecommunication information working green, no Oct 2014

Mokhtar B, Azab M (2015) Survey on security issues in vehicular ad hoc networks. Alexndria Eng J 54(4):1115–1126. https://doi.org/10.1016/j.aej.2015.07.011

Nahri M, Boulmakoul A, Karim L, Lbath A (2018) IoV distributed architecture for real-time traffic data analytics. Procedia Comput Sci 130:480–487. https://doi.org/10.1016/j.procs.2018.04.055

Priyan MK, Usha Devi G (2019) A survey on internet of vehicles: applications, technologies, challenges and opportunities. Int J Adv Intell Paradig 12(1–2):98–119. https://doi.org/10.1504/IJAIP.2019.096957

Qian Y, Moayeri N (2008) Design of secure and application-oriented vanets. In: IEEE vehicle technology conference, pp 2794–2799. https://doi.org/10.1109/VETECS.2008.610

Qu F, Wu Z, Wang F, Cho W (2015) A security and privacy review of VANETs. IEEE Trans Intell Transp Syst 16(6):2985–2996. https://doi.org/10.1109/TITS.2015.2439292

Renu SS, Saxena S (2020) Blockchain and UAV: security, challenges and research issues. In: Jain K, Khoshelham K, Zhu X, Tiwari A (eds) Proceedings of UASG 2019. UASG 2019. Lecture Notes in Civil Engineering, vol 51. Springer, Cham. https://doi.org/10.1007/978-3-030-37393-1_11

Sadiku MNO, Tembely M, Musa SM (2018) Internet of Vehicles: an introduction. Int J Adv Res Comput Sci Softw Eng 8(1):11. https://doi.org/10.23956/ijarcsse.v8i1.512

Sadio O, Ngom I, Lishou C (2018) Rethinking intelligent transportation systems with Internet of Vehicles: proposition of sensing as a service model. In: 2017 3rd IEEE international conference on computer communication, ICCC 2017, vol 2018-Jan, pp 2791–2796. https://doi.org/10.1109/CompComm.2017.8323041

Sharma S, Kaushik B (2000) A comprehensive review of nature-inspired algorithms for Internet of Vehicles. In: 2020 International conference on emerging smart computer informatics, ESCI 2020, pp 336–340. https://doi.org/10.1109/ESCI48226.2020.9167513

Sharma S, Kaushik B (2019) A survey on internet of vehicles: applications, security issues & solutions. Veh Commun 20:100182. https://doi.org/10.1016/j.vehcom.2019.100182

Sun Y et al (2017) Attacks and countermeasures in the internet of vehicles. Ann Des Telecommun Telecommun 72(5–6):283–295. https://doi.org/10.1007/s12243-016-0551-6

Tangade SS (2013) A survey on attacks, security and trust management solutions in VANETs, pp 2–7

Tuyisenge L, Ayaida M, Tohme S, Afilal LE (2018) Network architectures in Internet of Vehicles (IoV): review, protocols analysis, challenges and issues, vol 11253. Springer International Publishing, LNCS

Verroios V, Efstathiou V, Delis A (2011) Reaching available public parking spaces in urban environments using ad hoc networking. In: Proceedings of IEEE International Conference on Mobile Data Management, vol 1, pp 141–151. https://doi.org/10.1109/MDM.2011.49

Wan J, Liu J, Shao Z, Vasilakos AV, Imran M, Zhou K (2016) Mobile crowd sensing for traffic prediction in internet of vehicles. Sensors (switzerland) 16(1):1–15. https://doi.org/10.3390/s16010088

Wu W, Yang Z, Li K (2016) Internet of Vehicles and applications, pp 299–317. https://doi.org/10.1016/B978-0-12-805395-9/00016-2

Wunderlich R, Liu C, Elhanany I, Urbanik T (2008) A novel signal-scheduling algorithm with quality-of-service provisioning for an isolated intersection. IEEE Trans Intell Transp Syst 9(3):536–547. https://doi.org/10.1109/TITS.2008.928266

Yang F, Wang S, Li J, Liu Z, Sun Q (2014) An overview of Internet of Vehicles. China Commun 11(10):1–15. https://doi.org/10.1109/CC.2014.6969789

Zhang J, Letaief KB (2020) Mobile edge intelligence and computing for the Internet of Vehicles. Proc IEEE 108(2):246–261. https://doi.org/10.1109/JPROC.2019.2947490

Zheng K, Zheng Q, Chatzimisios P, Xiang W, Zhou Y (2015) Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions. IEEE Commun Surv Tutor 17(4):2377–2396. https://doi.org/10.1109/COMST.2015.2440103

Chapter 10
Cybersecurity and Ethics for IoT System: A Massive Analysis

Manish Thakral, Rishi Raj Singh, and Bharathi V. Kalghatgi

10.1 Introductıon

Cyberattacks have increased significantly as a result of the extreme and continuous rise in online interconnectivity, many of which have severe and devastating repercussions. Viruses are the most common method of obtaining malicious results in computers, regardless of whether the virus exploits weak spots or takes advantage of the many features of technological advancements (Manish 2021). Customers have made it clear that they need more robust and inventive antiparasitic organisms. As a starting point, we will discuss the common security breaches in new technology, firmware, and Internet protocol. Next, there is an explanation of the latest configuration avoidance, as well as why it works or does not work. Then, we will discuss new network threats based on innovations like Facebook, Twitter, virtualization, and connected devices. Lastly, we present our hypotheses about recent advances. Data centers and ICT products are now increasingly important to our culture, economy, and development. Cybercrime is becoming more appealing and more devastating as we rely more and more on software development. Similarly, according to a Kaspersky piracy study published in April 2012, the United States loses $114 billion each year to online assaults. The amount of cybercrime if the underlying reason for hacking attempts by businesses is included comes to an astonishing $385 billion. Additionally, the number of people who have been perpetrators has increased. In a Kaspersky research study of 100 children across countries and territories, 69% of respondents said they had been threatened online at some point in their lives (Ahmed and Broek 2017). According to Symantec, 14 adults are hacked every second, resulting in over a

M. Thakral (✉) · R. R. Singh
School of Computer Science UPES, Dehradun, India
e-mail: Manishthakra@gmail.com

B. V. Kalghatgi
ECE Department, Pes University, Bangalore, India
e-mail: BharathiV.Kalghatgi@pes.edu

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_10

thousand attempts per day. Safety involves gaining an understanding of the difficulties faced by cross-functional teams in regard to cybercrime and developing strategies (i.e., countermeasures) for maintaining the privacy, reliability, and access of almost any technology or technology sector. Confidential content is protected from being shared with unauthorized users or processes. Integrity means avoiding unwanted changes or deletions. Platforms can be used to move data, store information, and solve problems through capabilities known as usage. Many people who need them have access to them easily. According to military analysts, viruses are the most dangerous method of performing destructive breaches. There are attempts to protect privacy on the Web. Malicious software is a group of threats that are installed on a computer system to damage its core functions without the consent of its legal holder. Cybercrime encompasses infections, keyloggers, ransomware, bots, and pathogens as a whole. The installation of malware can be spread from compromised workstations, through poisoned email attachments, or by using memory cards to spread spyware. Viruses spread when they are entered into an IoT device and then spread to all other systems that use it in future. Sensor networks and digital logic would spread the infection. This study can be compromised by malware at any time, since computer viruses can be introduced at any time during the course of the study (Wright 2008). Malicious software might spread to servers through later computers. Supervisory system using packet-based management technologies, including Web servers (routes, changes, etc.) and control systems (e.g., wholesale prices, moves, etc.). Today, adware has become a pressing issue on the Web. Previously, cybercriminals took advantage of specific points of entry. For instance, computers, programs, or networks were used. At the edge routers, known flaws are exploited the entire time. Rather than safeguarding individual items, this comprehensive security method has primarily been used to create a barrier around all retained earnings to prevent outside intrusion. A preponderance of peripheral defense systems use firewalls and rim defense mechanisms. Surveillance cameras have been effectively bashed, according to studies. Any externally entered traffic will be captured, as well as a check to ensure a virus did not infiltrate the financial systems. Since securing one frontier is significantly simpler and appears to be cheaper than securing multiple perimeters, a defense paradigm has emerged that employs a significant number of individual computers or a vast amount of computation. According to authorities, network management methods have been deployed to provide more granular exposure to certain financial capabilities in conjunction with surrounding protective mechanisms. Figure 10.1 depicts the key elements and foundation key of cybersecurity (Portmann 2018).

Additionally, accountable is given alongside outer defensive and security controls to identify and correct any misdemeanors, as shown here. However, over time, the comprehensive security project's best effects have proven to be increasingly ineffective (Koch 2018). As ransomware evolves, it becomes more sophisticated. We discuss how adware that is continually changing tends to find ways to circumvent typical security measures. By looking at the gear, code, and Internet protocol, we propose a knowledge model. Since developing techniques have affected the way business is done, we chose a few to illustrate. Mobile devices, cloud services, social

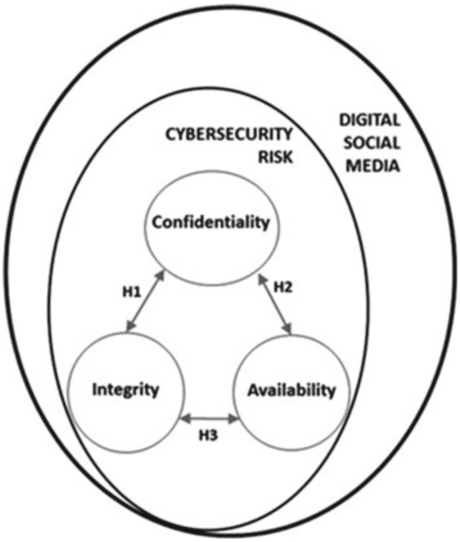


Fig. 10.1 Representation of cybersecurity Venn diagram

networking, and basic infrastructure are a few examples. Each of these latest techniques has distinct characteristics, and infection takes advantage of these qualities to spread. A lot of people are aware that online communication, such as blogs and online communities, has become an essential part of their daily lives. They talk about adolescent stress, give news, and make new friends. Figure 10.2 clearly depicts the cyber framework which is discussed in detail in the same section.

- Requirements related to information protection from unauthorized individuals or operations.

  Efficacy occurs when a program can prevent unnecessary alterations or deletions.

- The term "use" refers to the transfer, analysis, and solution of information.

Accessible to many people who use them, if they are also convenient. Worms are one of the most dangerous methods for carrying out damaging attacks, according to experts. Secrecy measures are being implemented on the Internet. A computer can be infected with spyware, which refers to a collection of threats. The goal of an

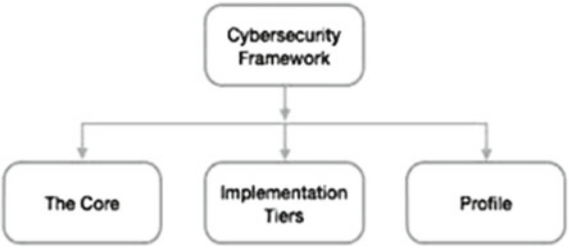


Fig. 10.2 Various functionalities of cybersecurity (deep learning neural network structure optimization 2020)

enemy with no knowledge of authorized ownership is to cause damage to the system. There are many types of malware in cyberspace, such as trojans, malware, and bots. It can use a variety of tactics to affect computers, including taking people away from infected machines, luring them to read infected messages, or convincing them to switch to a different computer user, for instance. Viruses can spread to many other platforms once they are installed on IoT workstations (deep learning neural network structure optimization 2020). According to journals, one virus can spread to many other platforms. The use of infectious smart objects and mathematical expressions in infrastructures should grow as technology advances. Adware is a form of software attack that can always be administered at any point as during the test's period, malicious code victims may spread to services via later-generation machines. Message company's ability, as well as network devices (e.g., paths, revisions, and on and on) plus power systems, is used by supervisory (e.g., wholesale prices, moves, etc.) (technology that can be programmed.) Adware's recent importance and complexity have become a major concern also on the Internet in recent years. Phishing emails used to operate from a single point of entry, such as a desktop, a software, or a networks. Confirmed operational faults are abused at every level at the network layer. Additionally, instead of securing each thing separately, this vulnerability management strategy has primarily been employed to create a barricade around all remaining income to ensure their protection. Any undesirable intrusion from the outside should be avoided. A report states that security video systems have been hacked in many external missile defense systems. A large number of external missile defense systems use IP tables and other border security methods. Any vehicle entering a building from the outside is recorded also double-checked how no hacker has compromised the banking sector. This method has found great acceptance. A security philosophy has formed, based on the fact that defending one boundary is much easier and tends to become less inexpensive than maintaining numerous zones. To have more precise visibility to particular money management skills, a large list of potential systems or a huge number of processing are used per the regulators, and net policy instruments were used in conjunction with encircling protection systems (Calcaterra et al. 2018). Moreover, as illustrated, accountability is provided alongside exterior reactive, and resources are made available to detect and correct any errors. As time passes, however, the maximum benefit of the vulnerability management effort has become less effective. Ransom is constantly evolving and becoming more complex. Software that constantly evolves has a tendency to circumvent surveillance systems, a comprehensive barrier to defense. We examine the most common malign influences in each of the science's key components. Figure 10.3 depicts the cybersecurity clause as blockchain which is already discussed in detail.

A knowing model is presented at the device, script, and backbone levels. Various features and disadvantages of the most suitable options are discussed. Allergies are a common occurrence in each of these stages. We describe a number of interesting pathogen common problems discovered in technological advances. Even though they have impacted how businesses are operated, we chose a few performance management practices to demonstrate. They affect social sharing, Web services, mobile

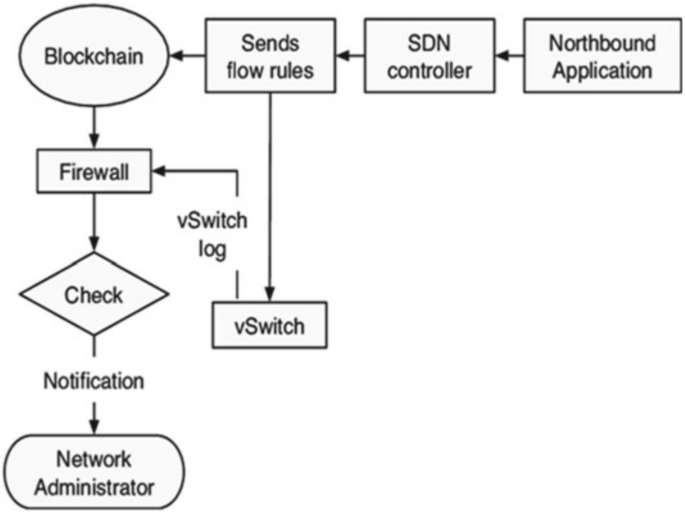


Fig. 10.3 Blockchain enables cybersecurity (Dinh and Thai 2018)

phones, and fundamental technology. We are discussing how sickness takes advantage of their unique characteristics to thrive. Here is a sample solution of the most recent approaches. For example, a lot of people are aware that instant messaging, such as virtual forums and blogs, has become a major part of life (Dinh and Thai 2018). People use it to lose weight concerning teenager pressures, provide updates, and build relationships. Utilizing the way to interact with hundreds of people simultaneously, adversaries are using email addresses to entrap naive individuals in an attempt to only use them for trashing private vehicles. Runtime modification of the criminal’s workstation enabled them to access the killer’s communications through the array serving system. Architecture, programming, and the Internet layer are the three layers of an allotted time frame. We discuss all the most significant methods of protection in these tiers and their advantages and disadvantages (Saxena et al. 2015).

Ransomware has evolved throughout history, using new techniques and exploiting technological advancements in order to evade capture. As part of this paper, we describe a variety of existing ransomware attackers found in developing technology. Since they affect the lives of people on a daily basis, we chose a few developing techniques to illustrate. Examples include digital networks, cloud services, mobile devices, and essential services. We describe the characteristics of some of these technological innovations, as well as how ransomware takes advantage of these characteristics. Our daily lives have become increasingly reliant on Internet sites, including social networking sites like blogs. Since many individuals use them to Weblog live lives, share headlines, and meet people. Antagonists deploy online profiles to connect unwitting individuals to use as automobiles for delivering spam to the killer’s acquaintances while the victim’s machine is transformed into a botnet, achieving the capacity to attract large numbers of people at once. The grid hosting approach enables customers to pay simply for what they use of network bandwidth, such as services, without having to maintain any capital expenditure or require any knowledge on how to manage sophisticated cloud platforms. As the amount of data stored in password managers grows, adversaries are becoming more interested. In June 2012, terrorists gained access to the denial-of-service (DDoS) system. Cloud Flare's (DDoS) prevention software exploited weaknesses in AT&T's mail network targeting telephone services; similarly, Google's email clients can use its billing function. By 2015, there will be 2 billion users worldwide, according to forecasts. In recent years, there has been a considerable increase in ransomware attacks. Adware for smartphone grew two times in 2012 compared to the prior year. Concerns are also mounting terrorist attacks, damage, and data breaches to transportation system such as communications networks and medical systems as well as data warfare aside from looking for malpractices based on specific qualities in the designated emerging economies. Humans also examine basic virus offensive hidden patterns between them to properly appreciate the strategies and tendencies of the ransomware attacks new assaults (Ozturan 2020).

As a general overview of the article, the following structure is used. The second section examines the virus in more detail. The second paragraph explains how adware is spreading into current systems, as well as possible mitigation mechanisms. Chapter four explores new virus approaches and explores common attack tactics, followed by chapter five, which summarizes the next study possibilities we selected, and chapter six concludes (Liu and Ding 2021).

10.2 Frequently used to Attack Official or Employment Agencies

To obtain classified information one can go for ransomware analysis. There are also cases where ransomware is used on individuals. Job applications and banking information represent a few examples of qualitative data. Antivirus software has gradually been improved not just to encrypt content, but also to connect faster to networks.

Not for profit solely. The vast majority of viruses were created with the intention of gaining power. According to the Global Pro Group, these viruses are used to generate phishing emails, analyze video streaming habits, and distribute uninvited materials. In 2012, spyware was found in the wild. Viruses represent almost half of all modern attacks, as per the images in the chart showing the refractive indexes of the different types of modern infected machines. This percentage is steadily increasing. The Generally Pro team defined the problems by reviewing the entire first half of 2012. The number of new infections caused by viruses was estimated to be 60% in 2009. As of 2011 at 73%, the percentage has increased. About two out of four new computer viruses are caused by viruses. Rogue versions of malware were created in 2011, showing that cyberattackers could work around physical assets and incursion to transmit viruses. Most attacks involve junk mail, fraud, and illegal downloads. Sending out junk communication to thousands or millions around the world that is unrelated, unethical, and uninvited is known as junk. When spammers are sent indiscriminately and without any sort of fee, it is a huge business. The amount of wireless Internet access is immense, and there are plenty of hackers taking advantage of low barriers to entry. The volume of letters has significantly increased over the past decade. It is estimated that over six million spam emails will be sent in 2011. In addition to reduced workdays and dishonesty, email requires additional capacity. On Thursday, spam is easiest to recognize. 88–92% of work emails sent in the first semester of 2010 were spam according to results of the text professional project team. Deception is a technique to obtain confidential information, such as a username, account number, or username, by pretending to be someone else. The majority of email schemes work by tricking users into accessing an infected URL. Posing as representatives of legitimate corporations. The unwitting entry of personal information into a fraudulent Website. A most phishing attacks use mechanical extortion platforms to exploit financial institutions. A phishing attack involves tricking a prepaid account into sending a verification email (and mimicking its domain) to a government agency. Sites and URLs are frequently misspelled in attacks. Rightwing program according to a technical analysis phishers in 2011 avoided using the word "phishing" to hide their intentions. To display their bogus strong passwords, they use a known IP address. In this case, the phishing attacks used a hacked address in order to avoid being discovered. According to reports, the amount of spammers using the falsified domain has decreased by 16%. As consumers become more educated, fraudsters are becoming more proficient at knowing the characteristics of a regular swamp—Unintentional infections due to cars driving are increasingly common. Adware sits are installed by criminals, sometimes when a person is browsing the Web, visiting a homepage, and when they view email or click on a deceptive shake display. The majority of fly transfers occur when data are shared between organizations. Your computer has been infiltrated by various ransomware types. There are more and more Websites being created. According to the hierarchy of criteria intelligence, there are four million pathogen varieties. In 2008, 90% of the software had been identified, and 90% of its users installed it from well-known and well-trusted Websites. Before downloading anything, a user must first browse the infected Website. The goal of phishing emails is to persuade the user to visit a dangerous site. Phishing emails can be used to spread harmful material on blogs. In addition, when a customer accesses a rogue domain, the customer downloads a virus without the defendant's awareness. The famous motor, for instance, is spreading malicious software with email notifications (Subramanian 2019).

10.3 Taking Advantage of Known Flaws

Identity thieves can use ransomware's existing features to steal information after it is installed on victims' computers. They can continue exploiting platform weaknesses in order to employ them for nefarious purposes (Zheng et al. 2019). In this post, we examine the most common ways that people are abused by technology, devices, and Internet connections. Following this, we will discuss the current activities that have been proposed as a means to reduce the harmful effects of the malpractices. Below is a list of the most prevalent incidents as depicted by the physical, programming, and Internet protocols, as well as examples of responses (Baltrusaitis et al. 2019).

10.3.1 Equipment

It is the equipment in a virtual machine that has the greatest power to control it. This is the level of difficulty. If the vulnerability is exploited, it gives criminals a lot of freedom and capacity to commit harmful offensive assaults. Devices have been tampered with. In terms of software-based attacks, there are several security updates and vulnerability scanners on the market. Although pro-Trump devices are continuously monitored to block various vulnerabilities, many electronics attacks are still possible at rest or in transit. A lot of electronic vulnerabilities have been observed on the emergence of software, turning away the pressure of tools that support operating system identification. The chipset virus is probably the most heinous of the various items of equipment abuse. The equipment computer viruses are fraudulent and purposefully undetectable modifications to electrical appliances like honesty. In silicon, there are electronic components (ICs). The equipment trojans come in all sorts of diplomas, each of which causes a bunch of problems implications (Fioretto et al. 2018). A piece of technology and a channel estimation module could be influenced by a computer virus to recognize arguments that should really be ignored. More configurations in the software's interconnectedness could mean so much battery capacity, which would completely consume the power pack. Alternatively, denial-of-service (DoS) attacks prevent something from functioning. Denial-of-service (DoS) trojans can damage a computer.

Disabling devices' public resources, including their processing power, their processing, and their batteries. A device's settings can also be changed for medical research purposes. The chances of harmful backdoors or electronics hackers getting access to technology are increasing. One way to improve efficiency is to convince the CPU to ignore interrupts coming from one device by changing, disabling, or destroying the device's settings. As a result of business organizations looking to cut costs, offer and drive out untrustworthy vendors, the opportunity to create non-authentic devices has increased (Sahil and Sood 2021). As a result of the modern IT leasing paradigm, Karri et al. highlight how items purchased from shopping Websites could be obtained from untrustworthy international companies by using modified hard drives. Business organizations frequently purchase untrustworthy gear, such as graphics cards and distributors, which can harbor dangerous device infections. Additionally, these actions increase the risks of compromise of underlying devices and are troublesome for IT organizations involved in compromised equipment. The theoretical constructs of the software will be accessible to unapproved people. When an enemy examines a device's outputs, a method called attack detection, they can learn about the device's brainwave patterns. They can also find out about physicochemical properties of the device, such as its storage capacity and Gamma rays are particles in the gamma range. There is a limit to the CPU usage of information in and out. As a result of all of these attacks on attack detection, sensitive information can be released. It examines a variety of ways in which encrypted data from a secure method can be discovered through RF power analysis. Various measures are taken to control the customer site. In order to protect the entire system as a whole, material that is impervious to tampering has become a major issue. The technology package (TPM) includes symmetric cryptography and secure data storage, as well as the ability to exchange data that are tamper-proof and stored on Web servers SMP (trusted platform base) refers to a system that has features of both computing devices and its platform that are critical to its physical functionality. A TCB should never contain errors or weaknesses, as these coulds compromise the cybersecurity of the overall system. Using microprocessor analysis, the company's cause of physical abuse is thoroughly examined (Singh et al. 2020). To ensure the confidentiality of, program audits. Electronic steganography hides registration information in circuit descriptions in order to restrict counterfeiting of the host item. Machinery vagueness is a method for concealing platforms by altering their design or construction. You use these to stop counterfeiters from getting their hands on the original design. Or how to copy critical network devices like IC modules. Any of the solutions that can be used to counteract encompasses a range background noise are introduced so that real knowledge cannot be exhibited directly, and some sections of the data are filtered assess alternative, as well as attempting to make, which aims to eliminate any association between the process parameters and side sensor nodes (Panarello et al. 2018).

10.3.2 Errors in Software

A design flaw is a word used to indicate an accident, shortcoming, miscalculation, or problem in a computer algorithm such as Microsoft Office. Working with proprietary operating systems, independent devices, and middleware cybersecurity threats exploits program flaws to have devices say and do things that are unanticipated and against their intended promise (Christidis and Devetsikiotis 2016).

Today, attackers still try to exploit security flaws and malfunctioning equipment to launch attacks. When certain elements of the widget toolkit and interaction are used, this is known as browser abuse. The most typical way to create computer viruses and login capability to users is by exploiting software defects in the cache, user input processing, and race situations. It is very common for hackers to manipulate a computer spot's memory by changing false positives on disks. A buffer overflow occurs when too much data are stored in practice. More information than a cushion can truly hold is a bad idea. Data processing in buffers is wasted because they hold only a limited amount of information. It is possible to flood information into nearby files, destroying or altering the original data. The attacker can manipulate process management code by ensuring that input features conform to specific rules. Security breaches can arise as the result of inaccurate inventory processing, such as in the case of session hijacking. Hacking is considered one of the best attacks. Exploiting a bug in Website technology is another well-known method. Applications are injected into the computer database through an attack (Neudecker and Hartenstein 2019). This could potentially result in SQL queries being changed, or even providing an attacker with access to data such as bank account details or usernames. The evaluation error is another name for manipulating the review. A common problem is the confusion of privileges. Exploiting a defect can lead a number of companies dominated by providing infrastructure have already begun to impact outcomes. As a result, the highest ranked enemies can obtain and commit crimes, since the password hashes of applications and users are safeguarded. This is a primary goal (Huang and Tan 2009). These companies are not focused on resolving legal issues but are more concerned with their major priority. These initiatives are meant to generate concepts for the establishment of private computer platforms. We are developing security testing approaches, educating system administrators, and advancing the status of the industry in terms of information security through the use of process developed reviews. The analysis and rearrangement of data are two of the most extensively used techniques for making sure computers do not breach vernacular encryption practices. It is one of the most common types of screening that occurs before the program begins. The system checks for dangerous types of items before it begins. Decentralizing the application and conducting execution checks is one good way to modify the application in a manner that prevents the program from being changed in a discriminatory way. The aim of deceit is to create difficult-to-understand code and integer arithmetic (van Oorschot 2020).

10.3.3 Security Vulnerability in Internet Services and Protocols

It is difficult to utilize scales effectively in several situations in which it is used today due to a completely different style of authentication from that utilized then. Both IT administrators are unfamiliar with connectivity, making link layer flaws difficult to diagnose. A popular DDoS attack is to attempt to exploit other businesses' operating systems restrictions to launch a DDoS attack. An effective encrypted file is not used; suggested updates are not kept up to date; or ignored. In addition to installation procedures and screens, there are a number of network protocols such as the World Wide Web standard (SIP), data channel (Http), or hostname (Drp). Protocol layer (IP) is most commonly used for the routing of packets between routers and computers. IP originally did not have a means of securing data integrity and privacy. During transmission between two devices over an unknown network, data could be intercepted or modified. TDomain names are converted into 32-bit email accounts by using the acceptance of online (DNS) process (Uriarte and DeNicola 2018).

A URL is a reference book for network, instructing gateways which fig system to use for packaging material. Using this vulnerability, an attacker can send harmful communications through the DNS by making it appear that they are official even though they are using an unverified server. Another issue is the lack of who is information (Dinh et al. 2018). A devastating attack on DHCP has been responsible for a substantial disruption to the online did it did (denial-of-service) operations. Confidentiality is an important tool for ensuring data are encrypted and only others with the necessary keys can decode it. A common method of securing data is encryption. A survey conducted by the cybersecurity association in 2007 found that 71% of businesses used encrypted material throughout the shipping process to safeguard advanced detection attacks that exploit cryptography's weaknesses. The use of analytics has also increased a wide range of activities. To tackle this problem, networking experts and visualizing specialists have teamed up. New methods for viewing connected data are being explored. A computer examines the database's display. Companies have partnered with professionals in the computational model as shown in Fig. 10.4. Since there are various programs and plans to address problems at the device, software, and component levels, instead of relying on each practice. The protection of all external assets from threats is also more effective by using integrated threat mitigation strategies (Sureshkumar and Vijayakumar 2020).

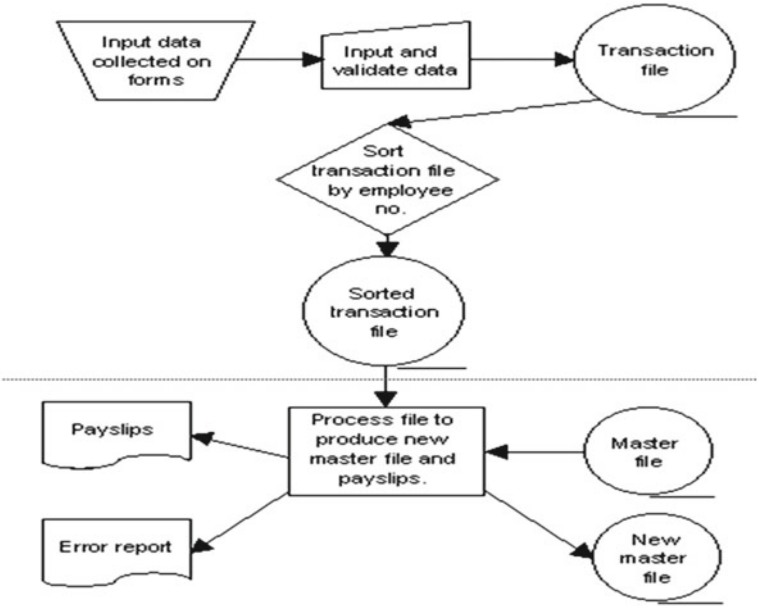

Input data collected on forms
Input and validate data
Transaction file
Sort transaction file by employee no.
Sorted transaction file
Payslips
Process file to produce new master file and payslips.
Master file
Error report
New master file

Fig. 10.4 Data security in industry pay slips

Cyberattacks have been used in the usual fashion. A boundary defense is used by most businesses for physical security to protect personal devices from outside infiltration. Data are safeguarded by ramparts and barriers. NGFWs and vulnerability scanning are common technologies employed by international border services (IDS) effectively influencing IT assets, such as computers or special operations systems, are protected with containment or defense in depth tactics by the gate. The much more frequently applied solution for building small assets is encryption. Inbound and outbound traffic can be controlled by evaluating wireless signals and deciding whether to allow them through, based on a combination of also before the rules. A barrier can be installed at several levels of the Internet services. Firewalls, also known as IP addresses or IP addresses, run at the lowest level of the network and prevent packets from passing through. When they meet the requirements (i.e., settings) set by network management, the firewall will stop them (Singh et al. 2020). Despite the fact that many contemporary fortresses are extremely powerful, protocol stack gates cannot filter unwanted traffic, such as virus payloads. It makes use of proxy servers and port facilities. The implementation phase firewall monitors and sometimes blocks traffic. Inbound, production, or operationally defined calls that do not comply with the protocol stack firewall's established policy. In addition to serving as an intermediary, gateway servers make it possible for users to access various Websites software and listen to input messages (for example, connection queries). Other packets are blocked while this is occurring. Both application layer firewalls and proxies make it more difficult to compromise an internal system. Since attackers' capabilities and expertise have expanded, they have developed increasingly sophisticated methods for sending malicious files to a network of interest. For example, an attacker may take control of a publicly accessible device and use it as a weapon. For their own reasons, they use a VPN. The hacker produces packets with a fake network interface using the observed proxy with the intention of hiding the sender's identity or imitating another computing system. Any suspicious or unusual behavior on the network is filtered by intrusion detection systems (Lopes and Alexandre 2019). These detection systems are useful in that they aim to detect the early phases of an attack (for example, an attacker exploring a machine or a network) connection for specific weaknesses) and can subsequently assist in defending a system against the attack's succeeding stages. Also, these systems look for telltale signals of concerning the possible or patterns of activity, whether itis from a person, a service, or something else or a harmful piece of code that international and regional levels or other security systems may miss or disregard. In order to detect suspicious network packages, a variety of detection methods can be used. Fingerprinting or scans for unusual occurrences are two common ones. Authorization effect is described with the help of Fig. 10.5

The detecting system decides what constitutes regular traffic by studying patterns in real time and reporting anomalous traffic. Based on the object recognition, traffic behavior is predicted. The screening approach based on signatures has been deemed ineffective. In recent years, the number and skill of malware writers has expanded (Bhandari 2018). It is regarded as such. Machine learning technologies commonly utilized in the security industry make it nearly impossible to keep up with an ever absolute numerical. A template strategy modern unusual case sightings have been

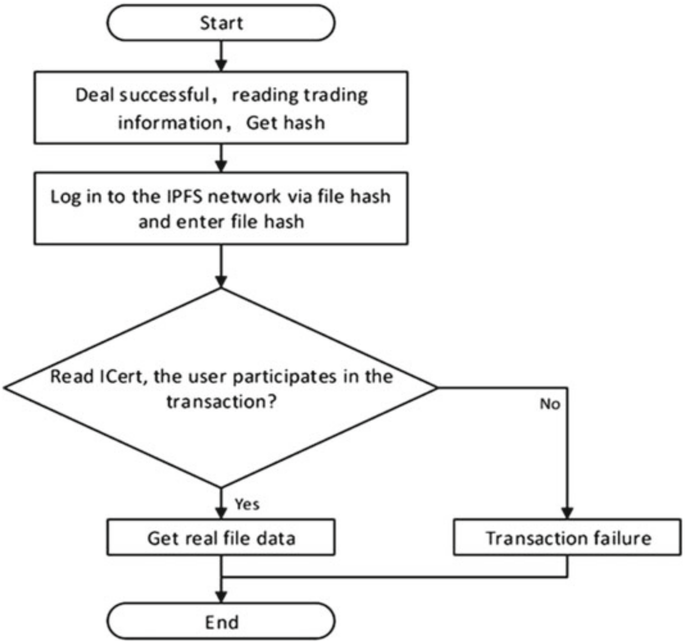

Start
Deal successful， reading trading information， Get hash
Log in to the IPFS network via file hash and enter file hash
Read ICert, the user participates in the transaction?
No
Yes
Get real file data
Transaction failure
End

Fig. 10.5 Authorization of transaction in banking industry

a hot topic in research. In this case, by analyzing communication for an extended time, the model learns by reference (ego) what defines ordinary. Investing time and developing a model of something like the analytical risks. As a malicious fingerprint, the procedure has evolved (identity). It determines regular traffic by analyzing real-time patterns and highlighting anomalous traffic. Based on object recognition, it predicts traffic behavior. It is possible to create better strategies to prevent undesirable communication information from new sites through the use of attack tactics, instead of focusing on individual components. Network forensics is the science of analyzing traffic through wiretaps on Wi-Fi. Web browsers, email, journals, online chat, and leader communications all fall under telnet. In court cases, the documentation is used for establishing a case, or to truly comprehend traffic flow vulnerabilities. eMailTrackerPro is a program that analyzes emails. The password of the device that followed orders is detected in the xml document, allowing the offender to be retrieved. For Internet browser flow forensics, applications like smart who is allow you to check up all of the accessible knowledge about a particular mobile device an email server, domain, or site that includes the continent, city or province, city, network insurer's name, and adviser's name as well as contact details for technical help. Web historian helps users evaluate Web page URLs some of which are saved in their browser the records of the past. The registry scanner is a comprehensive research with an emphasis that examines index .dat files to evaluate browser history and other information. A backdoor is a container in which honey is kept. A trapping is set to discover, intercept, or otherwise oppose efforts at unlawful material use. Any kind of knowledge shiplap ceiling lined data is used to discover more about the hazards that companies are facing or how to properly protect themselves threats. Numerous hackers are frequently hosted on a given biological phenomenon using digital methods. Therefore, even if the backdoor is hacked, there is a prospect for a sooner and less expensive recuperation. DoS attacks on a vast scale, due to insects, for example, have been used to observe a broader and more diversified network by connecting two or more intrusion detection systems on the same network connection. Cause serious damage is frequently used in conjunction with bigger detecting malware. A Kahlo is a type of farm that produces honey penetration testing and analytic tools in a centralized location (Sequeira and Gervasio 2020). Because universal distribution of resources is impossible, resources and services have now been employed to allow an ability to restrict access to only specific resources. The organizations that can conduct functions in the system are controlled by identity management.

10.4 Threats Are Already on the Rise

Breach of data on the Internet continues to evolve, adapting to the latest innovations. The characteristics of viruses can be adjusted to exploit vulnerabilities in emerging technologies. Others are used to further an individual's ambitions. New technology should be inspected for weaknesses that can harm systems. Benefiting from the new Internet (Schluse et al. 2018). Cybercrime relies on the widespread use of online resources, both by legitimate customers and criminal offenders. There was a significant death toll, and it was able to respond quickly and efficiently. Below are four new and exciting technological developments that could radically shift several industries. We recommend looking at Facebook, data storage, mobile devices, and strategic assets. Some of these technologies have significant vulnerabilities. To conduct a comprehensive study of any of these developments, we will describe and compare their individual characteristics. The number of widely used assault strategies is listed. Online security is featured in Fig. 10.6 gives clear flow of certification security (Barreiro et al. 2018).

10.4.1 Use of Social Media

New media platforms have contributed greatly to the growth of social media sites in recent months. There have been over 4 billion international registrations on social media since 2012 ended, but Zuckerberg has over 1.1 billion online accounts, a rate which is parabolic. There are over 1 billion Internet users worldwide. Internet usage has risen dramatically, and many young people now rely heavily on it for communication. Most social networking sites (such as Facebook, Instagram, LinkedIn, Pinterest,

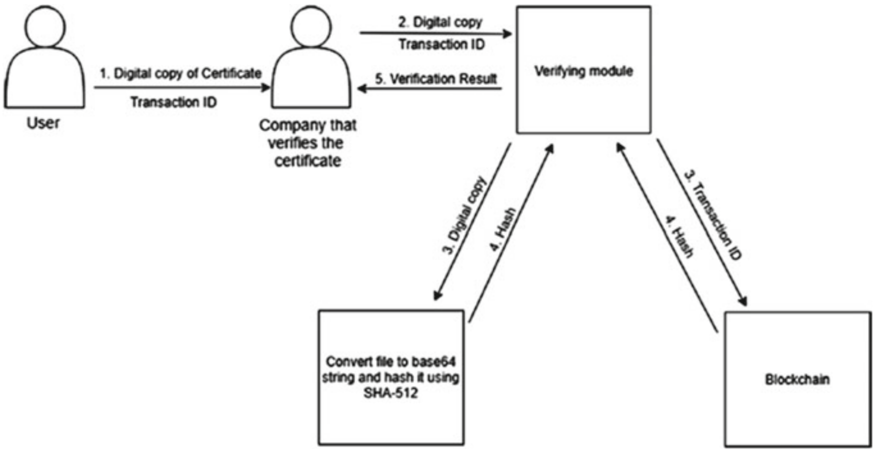


Fig. 10.6 Representation of data security flow in certification security

Tumblr, and Twitter) provide tools that allow customers to quickly express their feelings about relevant data (such as law, tackling, sex, place of birth, preferred songwriting, and new films), images, storylines, and links to other Web pages. Strikes are taking advantage of the popularity of the internet for using devious methods to their advantage. Thousands of harmful files, all related to social media sites, were found in the cybersecurity archive by the end of 2008. According to a cybersecurity firm named Sophos, social media attacks have significantly increased. Websites for entertainment according to every single report, approximately 60% of all social media groups have been spammed. Additionally, criminals can obtain additional information about customers by having access to publicly available business secrets.

The presence of links to social networks and the prominence of the brands they invest in concern more than 60% of businesses. People are creating new social networking accounts so that they can contact new users, and then spamming their friends with appealing links leading them to infected sites using the messages botnet. People put an end to cyberattacks, but then their photo sharing accounts are used as tools for spreading and perpetuating attacks, ultimately scamming the friends of the victims suspect's laptop as a vampire. It was created using Koobface as a model, and it successfully infiltrated the Web and detected malware zombies that were later used in legal prosecutions. Harmful URLs were distributed to 139 million networking site members, who shared them with 157,000 others, resulting in around 157,000 targets clicks people out of the online community. An unsavory virus was found to be included on numerous bHenry created it as a model. Conclusion: They concluded that individuals that blacklisted companies only have 27% accuracy. It was created using Koobface as a model, and it successfully infiltrated the Web and detected malware zombies that later became the basis for legal prosecutions, on average, readers of Kooface's spam have to wait four days before a response is made. Within the first two days, most photo sharing users are left unprotected. Other common flaws were discovered as well. An operation is initiated by using a large number of fake or dormant public social media pages. Computer perpetrators are devising more and more elaborate ways to seem reliable. Afterward, the crooks lure users to "companion" or follow other individuals on the Internet, e.g., and then click on their messages, often resulting in Web pages containing harmful codes. In a separate study, it was shown that a substantial number of reported infections occurred when users clicked on malicious links for popular Facebook themes like "progressing," being able to comprehend networking site networks and virus transmission mechanisms. Social media has also been used to investigate sneer services. Because of the concentration of numerous Websites, the proliferation of social networks has also increased the challenges of ensuring privacy combinations of different types of consumer data, as well as private information, and the conducted survey of data files are clearly labeled and organized. Online communities are appealing to a wide range of companies for this reason to try to accumulate enormous volumes of user results in order to achieve full load conditions for both lawful and illegitimate causes. In most circumstances, in many of those cases, people's level of protection is violated when personal data are extracted. A program's commitment to user privacy in NS depends on how individual users' data are stored. Suppliers have undergone extensive background checks tied to one's Facebook account, a method for encrypting confidential information posited by Lucas et al. Client-side JavaScript-based data no data are received by the online telecommunication companies thanks to this technology. A non-encrypted version hinders their ability to gather and store data that consumers divulge with the device. Networks are important for understanding users' privacy knowledge and providing useful tools that make it easier for users to adjust their privacy settings. This has also been considered. In another case, Ding + Gilovich introduced the concept of a confidentiality wizard. People are constantly being asked for additional input by the mentor. Classifiers are built by assigning privacy "labels" to acquaintances, and these labels are fed into a neural network model that uses artificial intelligence. The result is that additional rights are immediately assigned to the acquaintances of the user. Decision-makers It originated from the belief that privacy protection desires which acquaintances should really be authorized to see depend on actual usage informational data, which is derived from their long-standing and well-known patterns of behavior. The application will eventually reside on the VM and virtual operating system. PaaS enables programming environments to access and utilize additional application building blocks. Such programming environments have a visible impact on the application architecture, such as constraints on which the application can request services from an OS. Finally, in SaaS, t where the cloud providers control and manage user's data and services, forces the clients to have significant trust in their provider's technical competence. In cloud computing environments, the interactions between different service domains driven by service requirements are also dynamic, transient, and intensive (Manish et al. 2018). This suggests a need for an integrated, trust-based, secure interoperation framework that helps to establish, negotiate, and maintain trust to adaptively support policy integration (Vimal and Srivatsa 2019).

10.4.2 Data Storage System

Customers who save their data in the cloud continue to migrate to the big data cloud. One note and Facebook utilize email providers such as Google and live mail to manage email and keep track of their daily lives using other tools such as Mediafire and Siri. Myfitnesspal. Big data: The daily performance of the clouds must be computed by IT uniqueness and flexibility with big data using novel techniques information technology is characterized by having a reliable on-demand service automated provisioning, network-accessible, distributed user authentication, rapidly expandable, and peer. It is all about working effortlessly and clearly with the server (Smith n.d.). You can use no assets if you answer the question about embankments collectively used by various users, program, host, or platform level. Each client on the connection has access capabilities granted and changed as appropriate. When users have the ability to self-serve, an on-demand autonomous service is provided. You invest more money in social interaction, such as more space or faster processors. Once you have traveled a certain distance, the sky will be available as a resource, where customers pay based on how much they consume. Make utility payments, such as for energy, heat, and drinking. Another benefit of this technology is that it sends different products to the local tiers of both systems for customers. It makes use of several materials. In the generic Web application, the four tiers are as follows: We have divided the many layers of a computing system into the host machine, the design and appearance, the integrated data management, and the application server. The technology layer: This layer handles computer nodes and other natural facilities in the service network devices (e.g., firewalls, switching, electricity, and refrigeration devices). Machinery is used in data centers in practice. Normally, the heart of the data center consists of various servers, which are stacked on racks, coupled using switches, firewalls, or other technologies (Tran et al. 2012).

As far as the equipment layer is concerned, there are many difficulties that relate to the control panels, easy implementation, road safety, power, and so on. Managing resources to stay cool also termed as the VPN gateway, the development of information can be defined as a component which comprises computing as well as a host of other technologies. The core network makes available to a large amount of storage space. Using VMware vSphere, such as fusion, including the operator virtual disk (KVM), resource partitions can be applied to make computational resources available to virtual machine and the VMware software. It is responsible for a number of other functions. When you apply for network resource assignments, only Web applications can provide them. The Mac OS system components are as follows: The foundation layer is built at the top of the edge network, which is in turn based on the base layer foundations. The system layer's goal is to help software deployment as much as possible by using virtual machine (VM) frames. One example is cloud computing, which provides the APIs required to provide storage, servers, and other components on the Web server (AbuSamra et al. 2020).

Basic software product functionality

The access layer: This layer includes the microservices at the highest layer of your network. Software systems differ from regular programs in that they can maximize their potential through instantaneous capability. We get enhanced stability and are always available, and it costs less to operate. The Web supplies three primary categories of service: Saf (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). There are multiple data protection concerns for different platforms (as a service, PaaS) and equipment (as a service, IaaS) (Zhang et al. 2019). A cloud service provides virtual servers with specific challenges, such as operating systems (VMs) and memory. Clients can design and run programs using the servers. The software will run on the hypervisor and the real operating system, which will host the program. PaaS program extensions increase computer systems' access to comprehensive additional software tools proprietary and specialized computing platforms. Having a noticeable effect on software development is binding the components an OS component framework can use. Using micro in cloud services can better organize resources by spreading an equipment across several consumers by splitting the virtualization layer across data centers. Let us look at an example. They use desktops on the physical layer, but AWS uses query rewriters on the database server. Virtualization is an important emerging paradigm in this domain that abstracts services and technology for easy access. Customers can have their own virtual machines. VIO provides strong separation, indirect communication, and encrypted transactions between routers to provide strong segregation, direct sharing, and private information between VMs. Subjects of investigation guiding VM collection and sharing capabilities with a modular physical access method. Hosting is a possible solution to the problem. Clients since the use of software that has been acquired from separate providers is crucial. Vital considerations include using encrypted communications and making sure all the information used by those encrypted services is safe and sound. A PaaS platform, for instance, may restrict access to clearly defined areas of a hard disk, thus requiring users to request access to certain folders explicitly. Unexamined subject matter this exporting model is a really intriguing topic because it requires trust. Software companies handle clients' software and information, which forces customers to trust them. Expertise in specialized field interfaces in data centers that are linked by systems is expensive. Needs exhibit dynamic, transitory, and aggressive behavior too. Therefore, it has been claimed that trust must be developed in order to set up friendships and to manage respect, connections, and sharing that emerge from them (Marr 1977).

A new feature of the cloud is the necessary qualifications. This points to the necessity of having more problems, such as linguistic diversity, safe interconnection, and policy development control, which will need to be researched and tackled by this research area. Consumers' behavior might also change swiftly, which can have a dramatic effect on existing control messages. This is indicative of a trustworthy person identifying the reason structure proposed for the establishment, negotiation, and maintenance of trust. Using predictive analytics to help the economy grow (Blockchain and Artificial Intelligence Applications 2021).

10.4.3 Thoughtful Cell Phones

Wireless communication: there are more problems related to linguistic diversity, interconnection safety, and policy development control that need to be researched and addressed by this research area. Citation has improved significantly, and cellphones have combined with this to make an extremely powerful PC, a hand-held site access that is constantly being held by its owners. Confluence of increases in communication when it comes to structuring work life, offering control, individuality, and flexibility is a good choice. It is believed that over 50% of people use a smartphone daily, and it is projected that about 2 billion people own a tablet. Every person on the planet will have a cellphone by the end of 2013. In addition to basic social networking, store a lot of confidential information. Within shaping business processes, technological advances are having substantial impacts on the structure of these systems, and as a result, develop into additional sources of risk. The issue of privacy has gotten worse. Individuals' information and the company's creative property must be kept under strict control to ensure their safety. As digital phones have expanded exponentially, cybercriminals have found an enticing target. The threat of security issues looms. When it comes to the issues faced by PCs and workplace computers, smartphones are different since they are integrated into every aspect of the data transmission process as well as a completely different operating context. The properties, specific to cloud gaming, are described by environmental compliance. Agility: This is one of the most significant cell phone characteristics. Smartphone users may easily take them with them wherever they go. With regard to mobility, there is a greater risk of theft, loss, or bodily harm when using mobile devices. High customization: Smartphones can be used individually as Linux machines. When cellphones are used to connect users over Wi-Fi networks, they are often capable of making provisions. Original free (Internet + data transfers) is used in this situation. Technological integration (McCloskey 2009): Cell phones have several core characteristics, including gaming. Media and information sharing, as well as Web surfing, use cloud computing. Business has transitioned to being more resource-constrained and capability-restricted. Mobile devices, in comparison with fixed ones, have four significant drawbacks. This computer's rechargeable battery is restricted, and its computational rights are protected. The screen size was reduced, and the keyboard keys were quite small inputs. When security software outgrows its nutrients and reaches its limits, problems arise. Threats are also often chosen because of the expansion of digital computing devices. Development and planning issues in cellular computing can result in interaction assaults substructure. The adversary might try to compromise the cell cable network security. It has now been proven that an encrypted application's security can be broken. 118 h in order to exploit the network (e.g., username, password). When cellphones are targeted, this type of assault is not uncommon, but in this case, cellphones are very vulnerable. There is only one way to communicate on the Web—Wi-Fi. Wi-Fi on mobile contains security concerns. Researchers have examined the devices, and they have found a variety of flaws. In contrast, the heat generated is a worm that grows over Wi-Fi, although not through a Bluetooth device empathy. The parasite delivers itself to the victim and looks for adjacent smartphones with Wi-Fi turned on, in turn, attached device. An application must be accepted by the user before installation may begin. The virus is installed after it is installed, and it attacks the PC. In order to avert interaction assaults, such as spying, cellular traffic is subject to monitoring, such as espionage either setting up forwarding nodes in the system or tracking any use of cellular technologies. Smart phones are vulnerable to another sort of attack which derives from weaknesses in the code itself, available on mobile devices. A Web browser is used to access the Internet. Like normal Internet browsers, smartphone Web pages have expanded from their original purpose of just doing online shopping with gadgets. Also, criminals employ plug-ins for malicious purposes, such as distributing viruses. It was completely because of the unlocked bootloader that people became aware of the smartphone a privilege escalation flaw in a module that is utilized by the Internet browser. In September 2009, developers found an exploitable vulnerability in the iPhone browser window by leveraging an outdated and insecure component. Attacks on cellular telephones can be malevolent, and these mobiles serve as a vehicle for threat actors. Advanced cyber scientists are competing for this position. Recently, Kaspersky danger investigations and CMSThreats threat assessments have warned of the rapid increase in infection. Also known as "Web optimization," it focuses on Android apps and Apple iPhone users, as these people use mobile devices to search on the Web. To scam, sellers use an ultimately responsible market as well as registration procedures. When publishing the service, process it. The centralized marketplace provides for the complete removal of any application if it is discovered to be suspect. Before the end customers download the material, it has already been generated. Apple uses a rigorous vetting procedure to guarantee all applications are in line. It must meet Apple's standards in order to be available on the App store encryption; the application has passed muster because of code signing with encryption element keys. The only option for Apple users to install programs is through the Mobile App. essentially the same as unfortunately, both Google's iPhone and the Android iOS also have a global bazaar where users can host programs. Nevertheless, unlike the phone, the Android app can be installed on more than one phone personality. Using crowdsourcing, software products are rated by users considered according to public complaints. The item is no longer available for purchase and will be deleted from the device once the removal process is completed. Mobile carriers utilize another strategy, which is different from the conventional technique (Colón 2018).

10.4.4 High-Value and Mission-Critical System

Vital importance in today's life centrality to the economy and social well-being are both critically important. On the basis of, it is generally agreed that a computer is similar to others. Essentially, it may be stated that key national facilities are at risk if communications and environmental attacks occur. The mathematical abstractions that are reliant on them are dependable and safe. New discoveries, as shown in published scientific, there have been investigations that have detailed a rising risk of force and Web assault on transmission motors or other important components of the power grid. Essential assets such as: Institutions that may be created include: Individuals or groups can commit terrorism as a means of stealing property for financial gain. Back-to-School Appeal India Grand Central and Taj Guesthouse were intentionally targeted by the terrorists with the words "bai attack." sabotaging people or individuals as such, including leftist organizations or countries that actively fight them, as well as environmentalists in an attempt. This is only an illustration of the fight against the climate, like when the airport in Tokyo was seized by protesters computer hackers for personal benefit, as well as nations launching attacks to get data. Damaging the transportation economy can also be part of terrorism. In the above case, an escalation of cyber threats was launched that brought down the site of the Estonia government. The nation's dispute with Russia inspired a number of demonstrations, which were engaged in by both the Tallinn government, various banks, departments, publications, and the media. In Russian, it is now impossible to see where the complex cemetery bazaars and combat burials from Soviet times once stood (Shenoy and Anupama 2018). A huge major catastrophe—whether it is a cyclone or an ordinary catastrophic event like a landslide, for example, can have an impact on public infrastructure like oil drilling, power, and water polygons. Strengthening the physical security of our nation's critical systems is a bigger challenge than strengthening the cybersecurity of our nation's entire ICT. Due to the extreme interconnectedness and complexity of these networks, a distinct challenge is often the result of perhaps. The electricity system in which geographically distributed production sites deliver power via voltage level stations located throughout the country. As the electricity moves down the line (from positive to negative voltage), eventually the energy will flow into human residences. All stages of manufacture and supply are located at these two locations. Controls in big structures are often managed by smart grid (SCADA) computers, which are networked to gaming consoles. Monitoring facilities and to the businesses administering the assets' company data (intranets) the intra-networks to assist in communicating with, for example, electricity controllers and end customers, the nodes are hooked up to the Internet. This list of links allow an attacker to exploit the system. Several workers use unauthorized connections to the embedded system for track maintenance, and occasionally. The service providers kept the computers' links going by using transmitters vendor-specific approaches and the prominence of commercial software and the usage of older vendor-specific approaches. Editions targeted at weaknesses are intended to introduce another layer in order to offer viable safeguards for the world's most important assets architecture Experts are already in the process of discovering the crucial platform's characteristics subsystems of construction. This entails comprehending system linkages as well as system robustness both essential assets, as well as detecting and measuring the ensuing impacts in a restricted period of time. In our daily lives, these devices rely on one another and have an immense number of users. Therefore, the vital infrastructure must always be up and running and with no drop or downturn in the 24-h system. The built-in feature allows for internal procedures such as pulses, contests, and military surveillance, and the recognition of every sign of non-operational tasks has been proposed (study, plans). Products are known as systems as a route to more automation an organized, synchronized reaction, and recuperation (Mitton and Simplot-Ryl 2014).

10.4.5 Energy Efficiency, Transportation Sustainability, Climate Change, and Affordable Housing

Cybersecurity is being increasingly discussed in embedded systems and sensors. Due to its increasing use in every aspect of our everyday lives, industry and academia are working more closely together. Embedded devices, such as those found in cars, appliances, smartphones, and other audio/video devices, are becoming increasingly common place existence. There exist reputation-damaging security problems in certain area. It has an extremely narrow mental trust limit and relies heavily on tactical security that are distinct from standard PC and corporate computer security challenges, both by virtue of their inherent nature and the actual department. Many connected devices and sensing devices have a low cost of operation. For example, storing a large cryptographic key on a small computer with limited storage is a good example. As a result, security products for enterprise use have no use in embedded software. Cameras and microcontrollers are both frequently found in integrated devices. Due to the physical size of an object, a single entity is restricted in how much energy, memory, processing power, and communication via put the entity can access. They rely heavily on tactical security and have an extremely narrow mental trust limit. One can look at homes and condominiums to see if they are present. Carrying spheres allows people to wield them in their fingers or wallets, offering several genetic techniques (Manish et al. 2019). They utilize when computers and other electronic devices are physically connected, frequently without the need for a Linux kernel, a deep link with operating systems can be formed. Various safety issues related to embedding devices, and smart phones have spawned multiple vulnerabilities. As a result, wearable devices are resistant to threats that exploit energy depletion. The microcontrollers are in the near vicinity of possible attackers, increasing the chances of attack scenarios where bodily access is required something must be done. Operations that use quantum objects as part of the attack are now possible because of this change. An illustration of an assault with regard to statistical methods is an operation on the network switch. To stay operational, integrated circuits must abide by rules that govern their behavior creative affliction: environmentally capable. Because of the extremely exposed work places of embedded devices, there is a significant risk of failure. Exhaustion is a weakness in an assault that causes the system to fail (or cause other environmental damage) encoded machine in order to reconfigure a stolen electronic machine. This mechanism is set up so it can be used for future mischief. It includes basic security and prohibiting unauthorized access in order to prevent illegal access. A critical part of keeping data safe and secure is the provision of secure user identification and strategies to protect the integrity of the data using found work and system security measures a critical component of the political environment. In most cases, the theoretical analysis does not need to be examined or altered to be important for deterring attacks. For example, the implementation may use approaches such as masks, window operations, and phony code inserts.72 theories have been put forward. When networking over Wi-Fi or cable connections is becoming more widespread for portable systems to provide systems to increase radio controlled data collecting and updating, the weaknesses that are exposed when these remotely controlled systems are compromised. A rising problem in the industry is the proliferation of malware and espionage. The word "Internet terrorism" describes actions that are racially biased in order to carry out damage and spying. Increased mental features a variety of ways criminals engage in cybercrime the tactics employed by a country to access another country's communications systems for the means of conducting combat as a result of which damage or inconvenience is caused. Generally, cybercrime is concerned with public security flaws and the sabotage of the infrastructure of other countries vital national architecture. The previous case dealt with intelligence gathering, which is a topic where highly secret documents are involved. This could violate global defense because unauthorized access has been monitored or changed. In the latter case, the emphasis is on: All centers, including the power grid and train industries, may be impacted. Back in 2009, The Department of Homeland Security (DHS) created a digital cyclone for the Department of Justice. The main goal of the activity was to test the country's ability to resist digital espionage shortcomings in the US military's plans for dealing with cyberattacks the cybersecurity weaknesses of the government. Following these technological advances, many scholars have suggested a variety of new goals. According to the strategic plan to defend the country's national digital infrastructure, a plan for identifying our nation's most important services has been offered. Computers that are connected are essential to a country's cyber defense, as well as any interrelationships between the computers. In order to safeguard our nation's vital infrastructure, we must first identify its vulnerabilities and then put in place mechanisms to mitigate their risks. It is being recommended that protection and response should be put in place.

References

Ahmed S, Broek N (2017) Blockchain could boost food security. Nature 550(7674):43–43

Baltrusaitis T, Ahuja C, Morency L (2019) Multimodal machine learning: a survey and taxonomy. IEEE Trans Pattern Anal Mach Intell 41(2):423–443

Barreiro E, Munteanu C, Cruz-Monteagudo M, Pazos A, González-Díaz H (2018) Net-Net auto machine learning (AutoML) prediction of complex ecosystems. Sci Rep 8(1).

Bhandari B (2018) Supply chain management, blockchains and smart contracts. SSRN Electron J

Calcaterra C, Kaal W, Andrei V (2018) Semada technical whitepaper—blockchain infrastructure for measuring domain specific reputation in autonomous decentralized and anonymous systems. SSRN Electron J

Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the Internet of Things. IEEE Access 4:2292–2303

Colón K (2018) Creating a patient-centered, global, decentralized health system: combining new payment and care delivery models with telemedicine, AI, and blockchain technology. Blockchain Healthcare Today 1:1–18

Deep Learning Neural Network Structure Optimization (2020) Informatics and applications

Dinh T, Thai M (2018) AI and blockchain: a disruptive integration. Computer 51(9):48–53

Dinh T, Liu R, Zhang M, Chen G, Ooi B, Wang J (2018) Untangling blockchain: a data processing view of blockchain systems. IEEE Trans Knowl Data Eng 30(7):1366–1385

Fioretto F, Pontelli E, Yeoh W (2018) Distributed constraint optimization problems and applications: a survey. J Artif Intell Res 61:623–698

Huang P, Tan L (2009) Design and implementation of partially decentralized P2P Botnet control server. J Comput Appl 29(9):2446–2449

Koch M (2018) Artificial intelligence is becoming natural. Cell 173(3):531–533

Liu B, Ding Z (2021) A consensus-based decentralized training algorithm for deep neural networks with communication compression. Neurocomputing 440:287–296

Lopes V, Alexandre L (2019) An overview of blockchain integration with robotics and artificial intelligence. Ledger

Marr D (1977) Artificial intelligence—a personal view. Artif Intell 9(1):37–48

McCloskey E (2009) The benefits of combining cohorts for mega-analysis. Bone 44:S205

Melnik E, Klimenko A, Ivanov D (2019) A blockchain-based technique for making swarm robots distributed decisions. J Phys: Conf Ser 1333:052013

Mitton N, Simplot-Ryl D (2014) Wireless sensor and robot networks. World Scientific Pub. Co., Singapore

Neudecker T, Hartenstein H (2019) Network layer aspects of permissionless blockchains. IEEE Commun Surv Tutor 21(1):838–857

Ozturan C (2020) Barter machine: an autonomous, distributed barter exchange on the ethereum blockchain. Ledger 5

Panarello A, Tapas N, Merlino G, Longo F, Puliafito A (2018) Blockchain and IoT integration: a systematic survey. Sensors 18(8):2575

Peng P, Tian Y, Xiang T, Wang Y, Pontil M, Huang T (2018) Joint semantic and latent attribute modelling for cross-class transfer learning. IEEE Trans Pattern Anal Mach Intell 40(7):1625–1638

Portmann E (2018) Rezension "blockchain: blueprint for a new economy". HMD Praxis der Wirtschaftsinformatik 55(6):1362–1364

Sahil, Sood S (2021) Smart vehicular traffic management: an edge cloud centric IoT based framework. Internet of Things 14:100140

Saxena S, Sanyal G, Sharma S, Yadav SK (2015) A new workflow model for energy efficient cloud tasks scheduling architecture. In: 2015 Second international conference on advances in computing and communication engineering, pp 21–27. https://doi.org/10.1109/ICACCE.2015.139

Schluse M, Priggemeyer M, Atorf L, Rossmann J (2018) Experimentable digital twins—streamlining simulation-based systems engineering for Industry 4.0. IEEE Trans Ind Inform 14(4):1722–1731

Sequeira P, Gervasio M (2020) Interesting elements for explainable reinforcement learning: understanding agents' capabilities and limitations. Artif Intell 288:103367

Shenoy M, Anupama KR (2018) Swarm-sync: a distributed global time synchronization framework for swarm robotic systems. Pervasive Mob Comput 44:1–30

Singh A, Alshehri M, Majumdar P, Mohammed AA, Kumar M, Abugabah A, Algarni A (2021) Machine learning and deep learning approaches against botnet attacks on internet of things network. Soft Comput. doi: 10.1007/s00500-021-06240-z

Singh RR, Thakral M, Kaushik S, Jain A, Chhabra G (2022) A blockchain-based expectation solution for the internet of bogus media. In: Hemanth DJ, Pelusi D, Vuppalapati C (eds) Intelligent data communication technologies and Internet of Things. Lecture notes on data engineering and communications technologies, vol 101. Springer, Singapore. https://doi.org/10.1007/978-981-16-7610-9_28

Singh B, Sharma K, Sharma N (2020) Blockchain applications, opportunities, challenges and risks: a survey. SSRN Electron J

Smith R (n.d.) Docker orchestration

Special Issue: Blockchain and Artificial Intelligence Applications (2021) Blockchain and artificial intelligence applications 1(2)

Srivastava S, Saxena S, Buyya RK, Kumar M, Shankar A, Bhushan B (2021) CGP: cluster-based gossip protocol for dynamic resource environment in cloud. Simul Model Pract Theory 108(April):102275. https://doi.org/10.1016/j.simpat.2021.102275

Sureshkumar T, Vijayakumar D (2020) Security in IoT networks using blockchain technology. J Adv Res Dyn Control Syst 12(1):74–79

Thakral M, Singh RR, Jain A, Chhabra G (2021) Rigid wrap ATM debit card fraud detection using multistage detection. In: 2021 6th international conference on signal processing, computing and control (ISPCC), 2021, pp 774–778. https://doi.org/10.1109/ISPCC53510.2021.9609521

Thakral M, Jain A, Kadyan V, Jain A (2021) An innovative intelligent solution incorporating artificial neural networks for medical diagnostic application. In: 2021 Sixth International Conference on Image Information Processing (ICIIP), pp 529–532. https://doi.org/10.1109/ICIIP53038.2021.9702631

Tran N, Chiang F, Li J (2012) Efficient cooperative backup with decentralized trust management. ACM Trans Storage 8(3):1–25

Uriarte R, DeNicola R (2018) Blockchain-based decentralized cloud/fog solutions: challenges, opportunities, and standards. IEEE Commun Stand Mag 2(3):22–28

van Oorschot P (2020) Blockchains and stealth tactics for teaching security. IEEE Secur Privacy 18(5):3–5

Vimal S, Srivatsa S (2019) A new cluster P2P file sharing system based on IPFS and blockchain technology. J Ambient Intell Hum Comput

Wright C (2008) Bitcoin: a peer-to-peer electronic cash system. SSRN Electron J

Zhang X, Grannis J, Baggili I, Beebe N (2019) Frameup: an incriminatory attack on Storj: a peer to peer blockchain enabled distributed storage system. Digit Investig 29:28–42

Zheng X, Zhu M, Li Q, Chen C, Tan Y (2019) FinBrain: when finance meets AI 2.0. Front Inf Technol Electron Eng 20(7):914–924

Chapter 11
Blockchain for Enhancing Security of IoT Devices

Yahye Adam Omar and S. B. Goyal

11.1 Introduction

In our current world, the use of emerging technologies has enormously expanded in society, improving many viewpoints of life status. These technologies have made improvements mainly due to the Internet's penetration, which has let large industries maintain the design and production of devices associated with people or with each other through the Internet. Devices are now performing better, and their dynamic communication with the human being enables these devices to be involved in most people's activities. In reality, most of these devices are not intense on individual use. Instead, they are engaged more in solving problems related to situations where hundreds or thousands of people meet (Sestino et al. 2020). The rate at which society contains results in technologies to perform activities that people often do not desire. In this case, the stability of controlling the improvement of activity is surrounded by devices that can do autonomously. These attributes of the devices make them part of the Internet of Things (IoT). Anything that can connect to the Internet, collect and share data can be categorized as part of the Internet of Things (Rouse 2019). We can represent it as a device that can collect data from its surroundings using sensors and actuators and transmit that data to the Internet, where it can be analyzed. The IoT enables multiple devices to connect through sensors and actuators that perform different tasks (Hendricks 2015). These tasks can be for private use or in vast environments such as campuses or cities. Their main duty is to collect information from the environment and perform a relative reaction (Yánez et al. 2020). IoT manages an environment's services through its structure, which mapped in layers and based on collecting information. The devices constantly sense the medium, which generates a large volume of data that serve as raw material for cloud computing (Othman and El-Mousa 2020). Although it offers unique advantages to improve user experience,

Y. A. Omar · S. B. Goyal (✉)
City University, Petaling Jaya, Malaysia
e-mail: sb.goyal@city.edu.my

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_11

IoT operation also presents several challenges, specifically data acquisition and data transmission. This puts users and company's data at risk. According to reports and research on IoT security, there are criteria in which security levels have been compromised, and data has been exploited (Alam et al. 2020). These limitations inhibit the development of this technology, which could revolutionize on the way we interact with our daily operations.

Many of the security imperfections observed in the IoT include manufacturers that drop back doors open to obtain information about the use of their products and thus improve their sales (Chioma 2020). Information management is currently a big issue that needs to be considered and prioritized in deploying any architecture that includes emerging technologies. Many regulations and standards are being worked on to preserve data security. Still, at the same time, it is necessary to look for models that ensure the proper use of information. Salient working features of Blockchain technology have raised the attraction to combine with IoT to handle information thoroughly and secure the user's identity from source to recipient. Blockchains clears the way for an IoT technology where legal services can be obtained and managed easily thoroughly in a democratic way (Tseng et al. 2020). In Blockchain network, there is no urgent need for trust, allowing more secured micro-transactions. In this work, we will describe the current challenges of IoT. We will also highlight the potential advantages of combining IoT with Blockchain to address these challenges. Various approaches for combining these two technologies will be proposed; finally, we will discover some benefits and drawbacks associate with the integration of IoT and Blockchain and discuss them accordingly.

11.1.1 IoT Challenges

The IoT has shown tremendous growth in the last few years. By 2025, it is being assumed that there will be above 30 billion IoT active devices connected to the Internet globally, and they have been widely used in smart manufacturing, smart wear, smart homes, etc. (Statista 2021). With the massive expansion in IoT devices, an immense amount of data is generated and collected, requiring extra management, control and security. IoT devices can observe, analyze and make intelligent decisions based on collected information; however, IoT devices' safety is not where it is supposed to be (Kim et al. 2020). Although many IoT manufacturers claim that their devices have been built with a robust security level and meet the challenges, we are finding in many cases that those claims are merely not valid. While there is a common belief that IoT could be the answer for several business challenges and enabler for many business opportunities, there are still several technical challenges that are striking globally IoT adoption. The following are brief introductions to these challenges:

11.1.1.1 Cyber-Attacks

IoT devices can store multiple credentials, e.g., manufacturer credential, provisioned during manufacturing and operational credentials established during commissioning; first-time use, ownership change, service change, etc. If the device is storing credentials, there is always a chance for an attacker to extract somehow it, which can compromise a device. Unlike the computers and laptops running a robust operating system with a fast processor, IoT devices have typically limited computational power and do not have security support built into it. In addition, IoT devices are cheap, facilitating an attacker to buy and attach probes for reverse engineering to learn how to attack the device. The following are common IoT attacks:

(a) *Distributed Denial of Service (DDoS)*

(DDoS) can make the services of a particular IT system unavailable (Rios et al. 2021). DDoS attacks can target IoT devices, IoT gateways, application services or cloud services by flooding them with requests affecting the service's availability to the point of complete denial of service. In order for an attacker to perform such an attack, he or she might need thousands of devices that are infected by his or her script code that tells those devices to start too many requests at the target website at a certain exact time.

(b) *Eavesdropping*

Eavesdropping is secretly listening to communications by an authorized party. IoT devices are typically interconnected devices creating a complex system that is continuously sharing data or actuating something. The sensitive information collected by the IoT devices could be exploited in case the IoT network has been penetrated.

(c) *BlueBone*

BlueBone is targeting Bluetooth devices exploiting Bluetooth vulnerability. The result could be the complete gain of unauthorized access to the targeted device. It does not require an attacker to pair with the Bluetooth device or be set on discoverable mode.

(d) *Jamming*

Jamming is when an attacker jams the signals to prevent devices from communicating with each other and the server. Jamming Wi-Fi signals or GPS is actually very easy to achieve, and it is very cheap as well.

(e) *Backdoor*

Backdoor is a particular kind of Trojan or virus clears the way for an attacker to re-enter the effected computer. Backdoor essentially opens a network port, command prompt or remote session that enables the attacker to get back into a targeted system at any point with no authentication. Backdoor permit the attacker to easily penetrate the target network, giving all the controls every single time and requiring not hacking the system again.

11.1.1.2 Privacy

The second challenge that faces IoT is data privacy. The network of IoT devices often refers to an extensive network and applications that are used to control the IoT devices. Data collected by the IoT devices mainly associated with their environment that they are operating in, which sometimes related to personal information. Individuals using IoT devices have different privacy expectations and may not be aware that IoT devices collect data about them and potentially share it with a third party (Weber 2010). The cryptographic approaches are something that IoT manufacturers do not consider that much, which is a crucial subject for sensitive data to be stored and transmitted through the Internet. As shown in reports (Porambage et al. 2016) 98 percent of data traffic transmitted by IoT devices through the Internet is unencrypted, which leads sensitive data such as personal information to be exposed on the network. IoT device manufacturers only settle about devices' overall functionality. Still, few of them think about adding required privacy layers. IoT devices are missing (privacy by design concepts) includes data integration, identification and authentication, which are critical for the data that involves people.

11.1.1.3 Interoperability

The third challenge with an IoT ecosystem is interoperability and standards (Noura et al. 2019). Traditional Internet is valued technology and considered the core one. It is the root for people to be connected and machines to interact and share their experience with the same protocols and standards. Due to the various heterogeneity of IoT protocols and standards, IoT face challenges when it integrated with another system. Interoperability helps the IoT quickly adopt the new techniques and applications and become more flexible to control and manage. For both organizational and individual users of IoT devices, interoperability can be an essential element as it helps to select devices with the appropriate features required for a particular application. It would be an easy question for IoT devices to connect to any other device or system and exchange information with interoperability. However, IoT manufacturers are flying blind, as there are no standards or common language (Mahda et al. 2017). The considerable interoperability issue in IoT devices can be considered a potential challenge that needs to be mitigated.

11.1.1.4 Massive Data Management

The fast development of IoT technology in different areas greatly impacted the quantity of data produced by IoT devices (Asad et al. 2017). In terms of amplification, storage or communication, it is tough to manage the massive data generated by IoT devices. The gigantic growing volume of data raises the necessity for a scalable infrastructure to manage it.

11.1.1.5 Device Identification

As the development of IoT technology continues, the information security team must implement techniques to manage heterogeneous devices and network access. IoT devices come in different forms and sizes. Device identification will be a considerable subject for IoT to interchange data and corporate with various applications. The necessity for solid device identification is high in IoT ecosystems, which is considering a primary challenge to adopt IoT technology.

11.1.1.6 Effective Traffic Shaping and Network Segmentation

In IoT ecosystem, transmission protocols, device type or sensitive data will trigger network segmentation policies. As IoT continue to evolve, we should anticipate discovering thousands of dynamically configured network segments. Providentially, this will not require VLAN tag configurations to be applied to all network switches. This gives us many abilities, especially when it comes to streaming and other things that do not choke on the Internet and prioritize what we need.

11.1.2 Mapping of IoT Vulnerabilities from High-Level to Low-Level, Indications and Solutions

See Table 11.1.

11.2 Blockchain Overview

Blockchain is one of the sensational technologies that is currently emerging. Blockchain redefines how we store, update and move data across networks, allowing an entirely new way to write and deploy applications. Blockchain can improve online security, trust and even create a new type of organization without hierarchy and centralized decision making (Janssen et al. 2020). In general, Blockchain consists of blocks attached in sequential order that make up the chain. Each block contains information. The concept of Blockchain was derived from Bitcoin cryptocurrency, but now the application of Blockchain far exceeds its original intention which is digital money and trusted data movement and storage (Miraz and Ali 2018). In addition, Blockchain braces the exchange of value (Internet of value). The working mechanism of Blockchain can enable composite solutions for computing challenges around security (Alam Khan et al. 2020). Participants of the Blockchain network treated inclusively and respected their privacy cryptographically. For that reason, it is expected to succeed the Internet in bringing about a tech revolution and radically

Table 11.1 Mapping of IoT vulnerabilities from high-to-low-level, indications and solutions

Types of IoT vulnerabilities from high-level to low-level effect					
No.	Vulnerability	Indication	Effected layer	Presented solution	References
1	Constrained Applied Protocol (CoAP) security issue with Internet	Denial of service, Network Bottleneck	Network Layer/Application layer	CoAP mapping/DLSHTTP TLS/filtration using 6LBR/Mirror Proxy (MP) and Resource Directory	(Brachmann et al. 2012)
2	Sybil attacks	Byzantine faults, unreliable broadcast, spamming, Privacy violation	Network layer	Analyzing user behavior, and maintaining lists of trusted/un-trusted users, Random walk on social graphs	(Zhang, et al. 2014)
3	Lack of Security Controls	No authentication or passwords	Transport layer, network layer	Strong encrypted password	(Granjal 2014)
4	Loopholes	Back doors	Network layer	Anti-malware solution and Network monitoring	(Micro 2018)
5	Exploitable Security control	Week encryption, encryption keys or passwords sent in clear text	Transport layer	Strong encryption Algorithm	(Raza et al. 2012)
6	Exploitable Hardware or Software Bugs	Buffer overflow attacks/Privilege escalation attacks	Application layer	Promptly patching and updating all the applications and the operating system	(Bekerman et al. 2020)

transform how humans share knowledge and materials by making them more ethical and dependable (Fig. 11.1).

Blockchain key elements are participants that create transactions and blocks that transactions are recorded in sequential order (Eris Industries Documentation 2016). Registration of a transaction in Blockchain requires to be maintained by all the participants in the network. First, they all have to check that the sequential order of the blocks is correct before attaching to the chain. Secondly, the computer that wins to solve the puzzle will present to the other participants in the network to verify the work (De Silva et al. 2021). Finally, the block will be added if all participants agree on the current situation of the Blockchain. This is a technique to escalate the integrity and build trust in the available data.

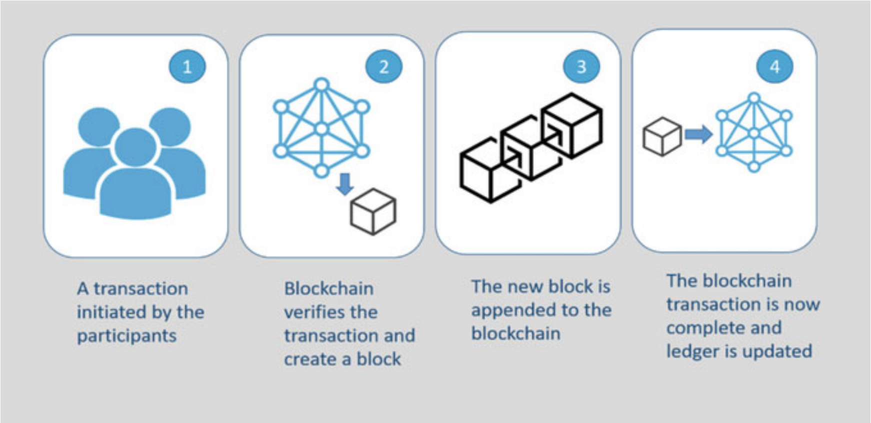

1
2
3
4
A transaction initiated by the participants
Blockchain verifies the transaction and create a block
The new block is appended to the blockchain
The blockchain transaction is now complete and ledger is updated

Fig. 11.1 How block of transactions created in blockchain

11.2.1 Types of Blockchain

The mainly three groups of Blockchain that exists are Public, Private and consortium Blockchain (Khettry et al. 2021). Based on their application use scenarios, they can be classified into their distinct attributes.

(a) *Public Blockchain*

Public Blockchains are entirely decentralized; it relies on the proof of work (PoW), a consensus algorithm that directs all participants to follow and obey one agreement. It is also open-source and not permissioned. Anyone who likes to be a participant in the network only needs to download the application's code and start validating the transactions without getting a permission from any source (C, 2018, p. 1). In addition, any individual around the world can see the ongoing transaction and participate in inserting his ones or validating them. Transactions are transparent but anonymous/pseudonymous. A perfect example of a public Blockchain network can be Bitcoin, Ethereum (Chow et al. 2021). Public Blockchain intended to maintain and accommodate various anonymous nodes. Therefore, it is highly demanded to have a reliable system and attenuate the potential risks. To solve a given puzzle, an expensive staking or computational power must take place in order to achieve the desired outcome. There must be a processing fee given to the rivals that solve the puzzle and add to the chain for every transaction. Tempering the information hosted by the public Blockchain is nearly impossible because it demands a high cost to attempt, thus preventing it from being hacked (Ch et al. 2020).

(b) *Private Blockchain*

Blockchain is said to be a private Blockchain if joining nodes are assented and are known members of a single organization (Yang et al. 2020). The Consensus rules only applied to a predetermined set of individuals. As a private Blockchain based on selected nodes, there is no urgent need for cryptography. There is no mining, proof of work or transaction fee in a private Blockchain, which ultimately differentiates from the public Blockchain. Typically, solitary enterprises utilize the private Blockchain as a synchronized distributed database to manage and track data in multiple departments. You might think about how private Blockchain be decentralized then. Technically, it is not. However, in private Blockchain platforms, there is a regulation that other platforms do not have. Therefore, all the nodes have to obey specific rules to ensure a company's proper flow. Since delegated nodes publish blocks within the network, a private Blockchain is faster because it will be less resource-intensive.

(c) *Consortium Blockchains*

We can find consortium Blockchain more similar to a private network. We can assume consortium Blockchain a kind of hybrid between public and private Blockchains. Even though it is a permissioned network, consortium Blockchain offer a decentralized structure. Each organization in this network receives similar treatment, which keeps things transparent and fair among the parties involved. There is no single entity ruling over the network. Multiple companies can collaborate using a consortium Blockchain and share data as well as maintaining the rules and records together.

11.2.2 Public and Private Key

Public key infrastructure (PKI) is one of the typical elements of Blockchain cryptography. This operation associated with two keys, a public and private. The public key is available and visible to any participant in the network, but the private key is only visible to its owner. For example, if you have a locked mailbox, the public key is the mailbox address; a person can insert money or a message into that mailbox but cannot retrieve it. The only way to retrieve the content is to use your private key. As long as no one can get that private key, the content will be kept secure for its owner. Whenever a private key is created, its public key is also generated from that private key (Komargodski and Segev 2020). A complex algorithm is processed to make the public key, but it is impossible to generate the private key from the public key. In other words, the process is uni-directional and impossible to reverse.

11.2.3 Digital Signature

The recorded data in the Blockchain needs integrity and desired security; one way to achieve that is by digital signature. Like the handwritten signature in the real-life world, a digital signature labels a unique mark to the digital data (Shahid and Khan 2020). Author's private key combined with the document that needs to be certified to reach its destination. In order to achieve the desired integrity, digital signature applies asymmetric cryptography for authentication and non-repudiation. When the receiver receives a message that applied a digital signature, the receiver can prove three things:

- The individual who is holding the public key applied to sign the letter, and that promotes authentication.
- If any variation attempted to the information or the sender's private key, a different signature will arise; therefore, to promote integrity and verify the legitimacy of the data, the receiver will use the public key and digital signature to retrieve the information from the sender.
- That the sender could prove these facts to a third party if necessary, and that is non-repudiation.

To utilize the advantages of digital signature, we must understand the public and private key concepts discussed in the previous section (see Fig. 11.2). Firstly, hash functions are collision-resistant. It is tough for a vital hash function to obtain the same two input that has the same output.

Secondly, to decrypt a key from asymmetric key pair, the other key from that pair is required. The public key is always used to encrypt the data and decrypt the data; the private key is used because we need only someone with a private key could read.

In the digital signature case, we reverse operation and use the private key for encryption and the public key for decryption (Damara et al. 2017). The goal is that we do not want to create a secret message, but instead, we need to create a secret message that a specific person with the private key could have only created. Anyone with the corresponding public key will merely then verify (Fig. 11.3).

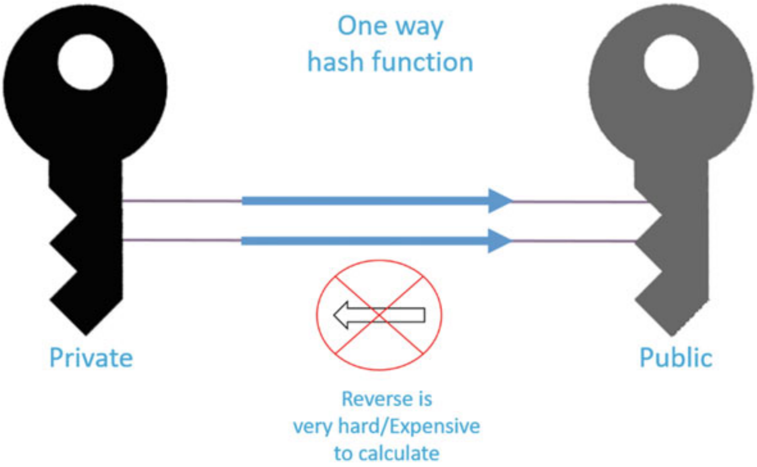


Fig. 11.2 Public and private key on the blockchain

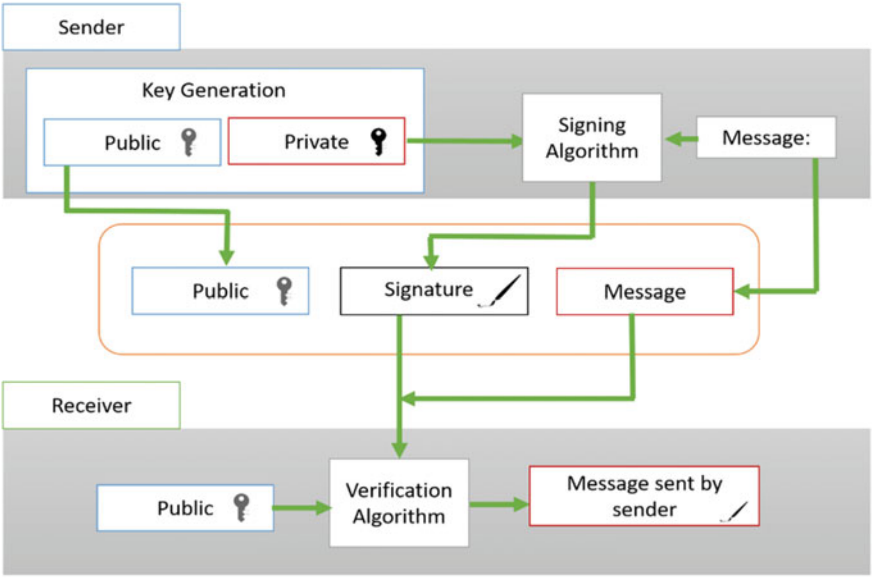


Fig. 11.3 Digital signature process

11.2.4 Smart Contract

A smart contract is a piece of software stored in the Blockchain that can be programmed to manage transactions to meet specific term and conditions (Androulaki et al. 2018). In other words, a smart contract introduces conditional logic to determine where transactions go. Unlike a traditional economic contract, a smart contract digitalizes the contract rules between various engaging entities. In Blockchain, the requirement for authentication to ensure that the smart contract's conditions are met is completely absent, which makes it the opposite of the traditional contracts enforced by a central authority. In the Blockchain, the smart contract will act as an agent that executes the transactions in a predetermined manner upon the network participant who agrees to the contract. For example, the contract between two parties will be converted into a computer language manner (code) that lies inside the Blockchain. Participants that involved are anonymous, but the contract is public to everyone on the Blockchain. Well-written smart contract can help us minimize the need for trust or intermediaries that manage the transaction between two parties. In a Blockchain network, smart contract facilitates algorithms that can process various functionalities and not only financial transactions.

- Loans can be offered automatically, and payment can occur at the same.
- Insurance companies can use it to process and claim their incidents more effectively.
- Delivery companies can use the smart contract to issue the payment for the sellers.

11.2.5 Consensus Algorithm

The consensus algorithm is a technique that allows all the participant in the Blockchain network to come to one agreement about the current state of the Blockchain. In this way, peers in the network achieve reliability from unknown participants (Foti et al. 2021, p. 116100). The consensus algorithm ensures that every new block to attach to the Blockchain has met all participants' desired conditions. The algorithms in consensus used so that the people in the decentralized distributed networks worldwide can play pretty and come to an agreement. Proper collaboration, equal rights and one single agreement are the objectives that Blockchain consensus protocols aim to maintain and regulate. Thus, a consensus algorithm tries to manage the standards and force the participant to obey a single agreement in the entire network. If a new block added to the Blockchain, the consensus mechanism must address the participant that will add to the Blockchain and make sure that this block is trustful and no one manipulates the data. The group of computers follow the strategy directed by the consensus to decide what is true. Most consensus algorithms on a public Blockchain share the same traits, including the cost of becoming a participant (resources), rewards and punishment. Anyone that participates fairly will receive a bonus (incentive). On the contrary, anyone who does not respect the rules or tries to attack the network will be penalized and lose that resource. In the following sections, we will discuss the most common consensus algorithms.

(a) *Proof of Work (PoW)*

Proof of Work (PoW) is a consensus algorithm that targets a miner for the next block generation. One of the environments used by the PoW consensus algorithm is Bitcoin. The basic working principle of this consensus algorithm is to work out a complex mathematical puzzle and give the appropriate result (Bach et al. 2018). A lot of computational power spent on solving the mathematical puzzle and the node that solves the puzzle will receive a reward, hence (incentive).

(b) *Proof of Stake (PoS)*

This algorithm is a common adequate substitution to PoW. The difference is that in this consensus algorithm, instead of spending a lot of computational power and computer resources to solve the mathematical problem and try to win the contest, people will stake actual coins. All the nodes will give support for validating the blocks. Once the node's stake is in place, the others will take part in the contest of which node will get forge the next block. In this case, the stakers forge the blocks; they do not mine them (Iansiti and Lakhani 2017). The winner of this contest is chosen by taking into consideration several factors such as how much money is being staked, how long the coins been staked for and randomization so that a single entity will gain a monopoly over forging.

(c) *Proof of Elapsed Time (PoET)*

In this algorithm, there is an equal chance of establishing the new block, unlike the PoW and PoS which the generation of the new block relies on all the participant; every validator on the network receives an equal chance to add a block in the chain. The permissioned Blockchain widely uses this consensus algorithm (Andriati 2020). This algorithm selects the next block using appropriate means, and that is why it is considered the most trustworthy consensus algorithm. All the nodes will have to wait a certain time to proof. The generated block will be presented to the others for further approval. The winner is the validator who has the most negligible timer value in the proof part.

11.2.6 Cryptography and Hashing

Cryptography is a technique applied to the data to prevent it from observing third parties who are not legitimate monitoring the data. Modern cryptography methods achieve complexity for saving the data using complex mathematical algorithms, computer science, physics, engineering and more (Ishmaev 2020). One great thing about cryptography is that altering any bit of data will ultimately produce a different output. For example, an output of (0000011) will be completely different from (0000012) and have no connection. Passwords are the most usage scenarios applied to cryptography. Most platforms keep the password in their hash form and look if the entered password matches to their stored hash form. If hackers successfully managed to penetrate the database, they will only receive the hashed form of the passwords, which will consider useless for them. Therefore, cryptographic hashing enables immutability (challenging to alter, resistant to change) for Blockchain technology. Hashing algorithms such as (SH-256), which is principally used by the Blockchain, have several advantages to the Blockchain (Table 11.2):

The hash functions play an important role in producing the new block and maintaining the structure of the chain. Besides, hash functions keep the data stored in the Blockchain secure and immutable. Any attempt for altering the data in the block will break the sequential order of the chain and point out the inconsistency. The Avalanche

Table 11.2 Benefits of cryptographic hash function in blockchain

Conveniences	Description
Distinctiveness	Every unique input will produce a unique output
Less time	Slight amount of time can be made from the output
Acceptance	Every input will have the same identical output in every time
Avalanche Effect	A bit change of the data can produce a massive difference
Row back effect	We cannot rebuild the input from the output, or vice versa

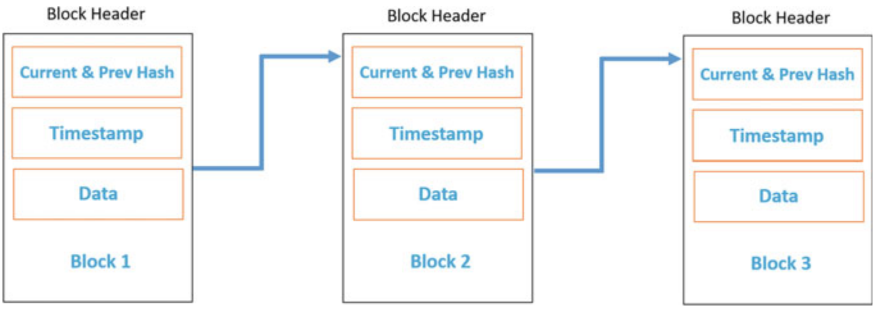


Fig. 11.4 Chain structure in blockchain

effect will arise if any irregular activity occurs to the data. Even if we make a slight change to the input, it will significantly impact the hash output compared to the original one (Fig. 11.4).

11.2.7 Identity Management

What gives Blockchain technology so convincing is that it has broad disruptive applications. We have already seen many possible uses in many industries. One of the most impressive and encouraging opportunities is identity management (Dixon 2017). It is a major societal, political, economic and computer science subject, and a full-proof technique of proving one's identity has been an intangible goal. Definitely, systems demand users to register their personal information, new credit and debit cards of embedded chips, and organizations use several other approaches to verify identity. However, several checks are required to ensure hundred percent integrity. Governments have afforded multiple tools for identity management, "passports and identity cards," and all have eventually failed as forgery-proof methods.

Identity theft and frauds are everyday things in our current world. The urgency for strong identity management becomes a critical thing, in a way that has never been ever. If we succeed to attenuate the risk, we are clearing the way for many new opportunities and innovations. Blockchain has awarded the solution of proper identity management. Some of the challenges that identity and access management want to address are things like regulation compliance, alleviating identity silos or securing APIs. Tempering with such public records can affect citizens, business and public services. By indexing the stored data with hashes, we can prevent such tampering. Through the core structure, the verifying individuals do not need to review the validity of the original data in the provided proof. Still, they can instead use the Blockchain to verify the attestation and attesting party (such as the government). They can determine whether to validate the proof (Khor et al. 2021).

11.3 Introduction to IoT and Blockchain

The Internet of Things (IoT) is shaping our lifestyle. IoT is a giant network with connected devices; these devices gather and share data about how they are used and the environment in which they employ. Objects such as automobile, medical devices and building automation are sensing and reacting, talking to us and each other. We can argue that everything connected to the Internet, collect and share data, is part of the IoT ecosystem.

Most IoT devices have the word smart at the start of their names; smartwatches, smart refrigerators, smart homes, etc. The IoT has already achieved considerable growth; however, the concept of the Internet of Things began in the early 1970s (Babu et al. 2016). Scientists rose to see the capability for interconnected information systems, mobile agility combined with location and energy-aware uses. Scientists invented the phrase pervasive computing or the embedded Internet. They imagine a computing environment where millions of computers would be incorporated into everything we use and talk to us and each other. The idea is that technology compounds so easily within our world that it essentially disappears (Fig. 11.5).

A device on the Internet of Things is an Internet-connected smart device. Unlike a computer that primarily intended to computes, the IoT design is to do a particular task like monitoring temperature or record video. The device gathers data and then transmits it to a remote location. Billions of intelligent devices make up the Internet of Things, from radios to refrigerators; they constantly communicate with us and to each other.

11.3.1 Real-Life Applications of IoT Devices

The IoT brings value to the business in various cities. It is transforming and improving sales by building predictive supply management and promoting customer satisfaction, employee productivity, innovation and asset utilization. While IoT can benefit

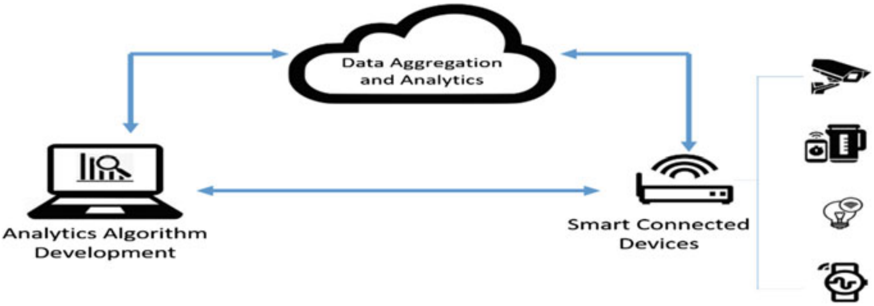

Data Aggregation and Analytics
Analytics Algorithm Development
Smart Connected Devices

Fig. 11.5 Generic IoT ecosystem

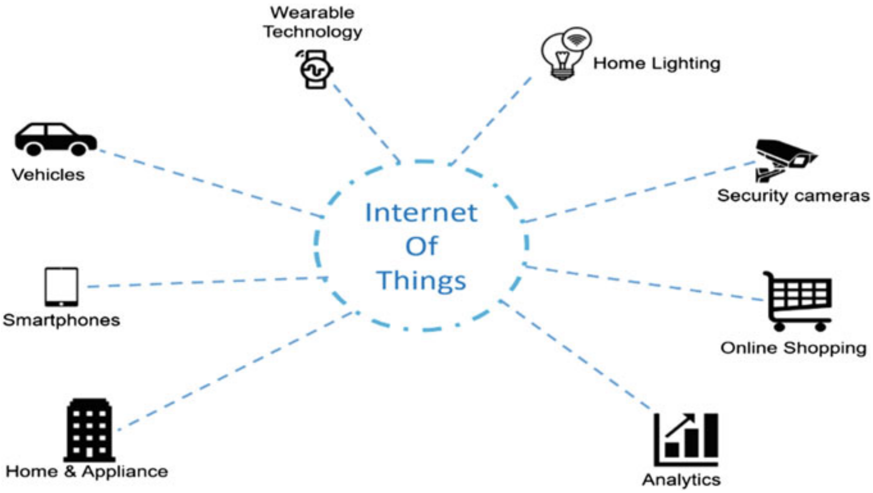


Fig. 11.6 IoT applications

most corporations, top participants include manufacturing, which is the leader at 40% of the IoT market. Advantages include reducing operating costs and creating a more dynamic inventory control. Healthcare has 30% of the IoT market. Departments use sensors to monitor patients and other devices to advance processes, patient experience and safety (Golosova and Romanovs 2018). Other industry players include retail. Business uses IoT devices to aid with inventory tracking. Sensors monitor customer movement and handle anonymous analytics of customer choices (Fig. 11.6).

In cities, the IoT can improve trash service by monitoring trash cans and notify garbage collectors only if the cans are full. Truckers then adjust the route to reduce fuel consumption. In education, teachers use radio-frequency identification (RFID) chips in ID cards to follow attendance. The justice systems integrate the IoT by providing wearable, embedded sensors to monitor and track the penitentiary complex's location. Security systems include remote motion sensors, biometric and facial locks. Whatever the business, there is value in the Internet of Things and will significantly impact production costs, prevent waste, delays and accelerate product design.

11.3.2 Real-Life Applications of Integration of IoT and Blockchain

With advancements in IoT, industries can obtain data, gain insight from the data and make decisions based on the data. The validity of the data receiving from the IoT devices is crucial, and typically we cannot make decisions from data that we cannot verify its source. IoT allows devices over the Internet to send data to

Table 11.3 IoT and blockchain use cases

No	Application	Description
1	Pharmaceutical	Patients, health data, new drugs, anticipating demand for treatment could enormously benefit from the integration IoT and Blockchain
2	Aviation	Real-time monitoring of sensitive elements such as turbine engines provide the optimal data foundation for predictive maintenance
3	Supply chain and logistics	Companies are composing the transportations IoT-enabled to track the movement throughout the shipment process. Due to the lack of transparency and difficulties in the current supply chain and logistics, Blockchain and IoT combined can improve the network's reliability and traceability

private Blockchain networks to build tamper-resistant records (Reyna et al. 2018). Blockchain enables a complete decentralized platform where business partners can access IoT data without the need for central control. Each transaction can be verified to prevent altercation and create trust among all permissioned network members.

IoT with Blockchain can deliver genuine trust to captured data (Zhu and Badr 2018). The fundamental point is to give devices, at the time of birth, an identity that can be approved and verified throughout their lifecycle with Blockchain. There is high potential for IoT systems in Blockchain technology capabilities that depend on device identity protocols and reputation systems. With device identity rules, each device can have its Blockchain public key and send encrypted challenge and response information to other devices, thereby ensuring a device remains in control of its identity. Besides, a device with an identity can develop a reputation or history tracked by a Blockchain. Several industries have begun to explore IoT and Blockchain's possible applications to advance efficiency and bring automation. The following are various Blockchain and IoT use cases (Table 11.3).

11.3.3 IoT Device Identity Management Through Blockchain

Digital identity can be used to represent an external agent that can be an organization, person, device or application. We can identify machines and systems digitally. The concept of giving digital identity is an essential component of the Internet of Things (Sinha and Pradhan 2021). The Internet of thing slowly becomes less of a future promise. Everyday household items such as, wearables, fridges or a watching machine come with a companion app and less of a novelty and more of an expectation at this point. This reality brings both a lot of convenience and risk into our everyday lives. This issue will only become further noticeable as more devices come online. Many of those challenges pertain to security. IoT has shown tremendous vulnerability and security breaches (Golosova and Romanovs 2018). However, the threat of hacking is not the only reason why the Identity of things (IDoT) is so important in smart devices. Devices need to be able to communicate, interact and built complex systems reliably. These requirements need to be met by products coming from various manufacturers and brands. Typical interactions that IoT devices need to manage are humans and machine (H2M), machine to machine (M2M) and machine to service interactions (M2SI).

Every single interaction needs and reaches its intended address. For example, if you have three smart plugs controlled with your smartphone and your IoT App cannot distinguish between them that is a mild inconvenience. The IPv4 addressing scalability was not considered and has recently run out of IP addresses to be assigned IoT devices. Managing the structure of IPv4 provides an insufficient number of publicly routable addresses to give a distinct lesson to every Internet device or service. This problem has been mitigated by changes in the address allocation and routing infrastructure of the Internet to IPv6, which provides a theoretical maximum of 3.4 × 1013 IP addresses (Chen et al. 2019). This vast address space enables the IoT's explosive growth, yet from a security perspective, managing IoT devices and users' identities remain a critical challenge. Although IPv6 provides a unique identification for every IoT device, proxies and DHCP play a considerable role in limiting the interoperability between IoT devices. There is an open direct relationship between IoT devices with people and other devices, and different people can access a device at varying amounts of time. Identity management involves processes related to authentication and authorization that are necessary to prevent users from accessing privileges.

11.4 Integration of IoT and Blockchain

The IoT is reshaping and streamlining manual procedures to make them part of the digital world. Besides, IoT provides huge volumes of data that companies can use to experience more in their profession and make better decision. In recent years, cloud computing technologies have provided the IoT with the necessary functionality to analyze and process information and utilize it in real-time actions and knowledge (Amin et al. 2018). This extraordinary growth in the IoT has initiated new community opportunities such as mechanisms to access and distribute information. The open data criterion is outstanding in these initiatives. However, one of the most significant vulnerabilities of these ambitions, as has occurred in many situations, is the lack of trust. Centralized architectures like the one used in cloud computing have remarkably contributed to the development of IoT. Though regarding data transparency, they act as black boxes, and network members do not have a clear insight into where and how the information they provide will be used. Moreover, centralized cloud services are vulnerable to faults and fatal security threats (Reyna et al. 2018). In the growth of IoT, the network edge is getting more functionality as corresponded to the cloud. The IoT can utilize the decentralized network models offered by Blockchains, so further expansions to the IoT can proceed while eliminating the need for trust in centralized services. However, Blockchains are still in their early stages of research and development, and there are still various research challenges regarding consistently integrating IoT and Blockchains. In this section, we will discuss about the major approaches to integrate both technologies to provide robust and secure environment for running IoT devices. We are going to start from the easiest way that we can utilize Blockchain features to make the data generated by the IoT more secure and less chance for intermediary attack.

11.4.1 Device Identity Approach

In this integration approach, each device connected to the system sign its own data and providing its own identity. The major difference between the traditional IoT architecture and Blockchain integrated architecture is that devices are now providing their identity and adding a digital signature to the data. Ultimately, the data cannot be altered while it travels across the middle services and reaches where it analyzed. This scheme broadly prevents man in the middle attack. By sending a cryptographically signed data with its device registered to the network, the data will be more secure and resistant to any point of leakage while traveling through the various middle service. Even if there is an intermediary attack when consuming the data, they will not be able to observe the private key of the devices, which makes is difficult to observe the data (Fig. 11.7).

This approach is the easiest way to integrate Blockchain features to the IoT. Here, we are not fully implementing the Blockchain working principles to the IoT, we merely using small portion, which is cryptographically signing the data before it leaves the source. This approach is not resistant to a single point of failure; however, it would be an interesting starting point for the integration.

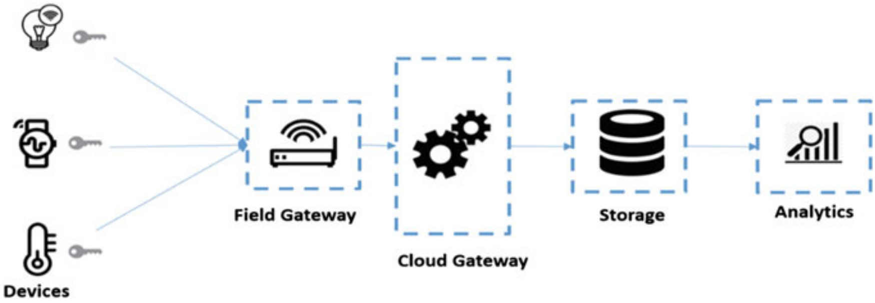


Fig. 11.7 Integration IoT and blockchain for device identity

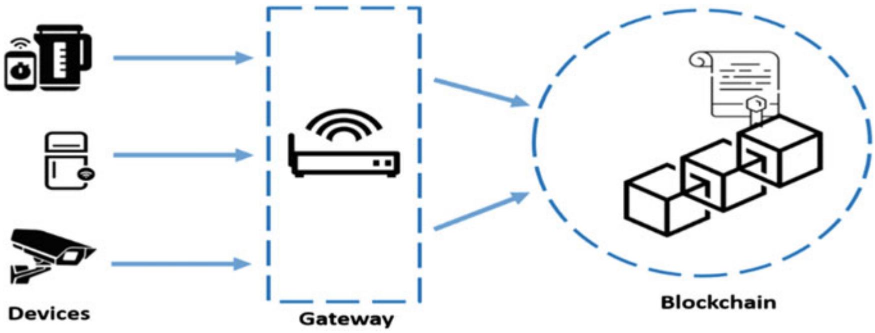


Fig. 11.8 Device gateway communication through blockchain

11.4.2 Device Gateway Communication Through Blockchain

In this scheme, all the interactions go to the Blockchain, enabling an immutable record of interactions. This integration method ensures that all the chosen activities are traceable as their details can be obtained in the Blockchain, and it improves the autonomy of IoT devices. IoT applications that assign to trade or rent, such as Slock, can leverage this method to provide their services. Nevertheless, recording all the Blockchain interactions would require an increase in bandwidth and data, which is one of the well-known challenges in Blockchain. On the other hand, all IoT data related to these transactions should also be stored in a Blockchain (Fig. 11.8).

The utilization of gateway will filter the data before it reaches to the Blockchain, this allows data easily absorbed by the Blockchain. The router will router the traffic enabling other to prevent other network traffic collision. This method is useful for many small and medium business, where data is collected for certain time to extract same basic decisions.

11.4.3 Peer-To-Peer IoT Blockchain-Based Integration Model

Figure 11.12 represents the process of combining IoT with Blockchain in a peer-to-peer design (P2P). This procedure is a fully decentralized system where every device is directly inscribing data to the Blockchain. Blockchain will serve as a middle layer between IoT and applications. Every device has a unique identity, which the Blockchain manages, ensuring a reliable approach to identify a specific source of any leakages and take quick remedial action (Yeow et al. 2018). The smart contract, which is the agreement of working governments among the network parties, ensures the Blockchain network's proper working mechanism, making data immutable (Hang and Kim 2019). The IoT Blockchain layer has all the modules

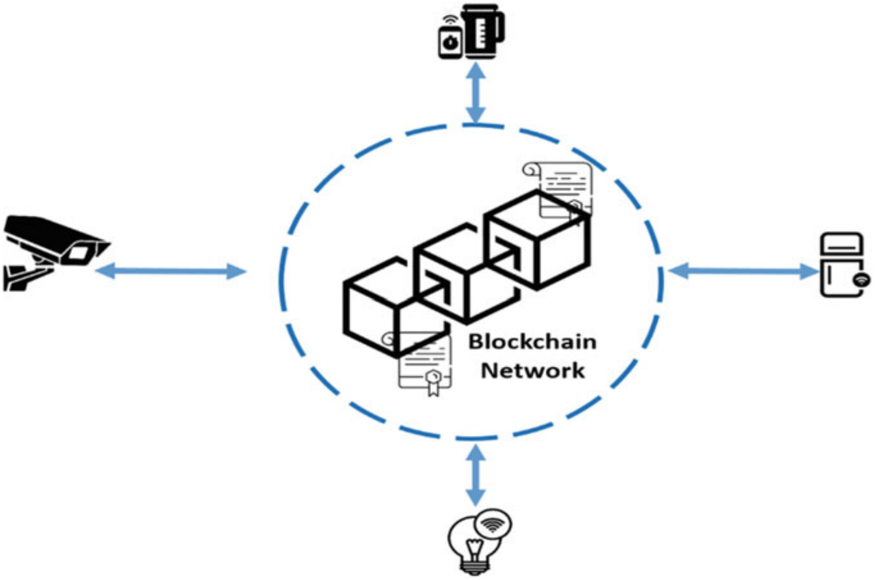


Fig. 11.9 Peer-to-Peer IoT blockchain-based integration model

to provide various Blockchain technology features, including peer-to-peer (P2P) communication, identity management and consensus (Fig. 11.9).

This approach expands the previous integration design, whereby IoT users decide to use the Blockchain for certain IoT interaction events, and the rest of the transactions transpire directly between IoT devices (Khan and Salah 2018). This approach leverages the benefits of decentralized record-keeping through Blockchains as well as real-time IoT delivery. Figure 11.13 is a representation of this hybrid integration approach. However, this approach optimizes the portion between the interactions that occur in real-time and those that go through the Blockchain. This allows critical core functions, compute, communicate, control, storage and decision making to be more accurate. This approach is very beneficial for areas where data latency, privacy and other data intensive issues are creating cost.

11.4.4 Hybrid Approach

This scheme intended to host only part of the Blockchain's interactions, and the rest are directly shared between the IoT devices. The main obstacle in this design is determining which interactions should go through the Blockchain and providing the way to decide this in run time. A perfect compose of this scheme would be the best way to combine both technologies since it supports Blockchain benefits and the benefits of real-time IoT interactions. In this model, fog computing could come into

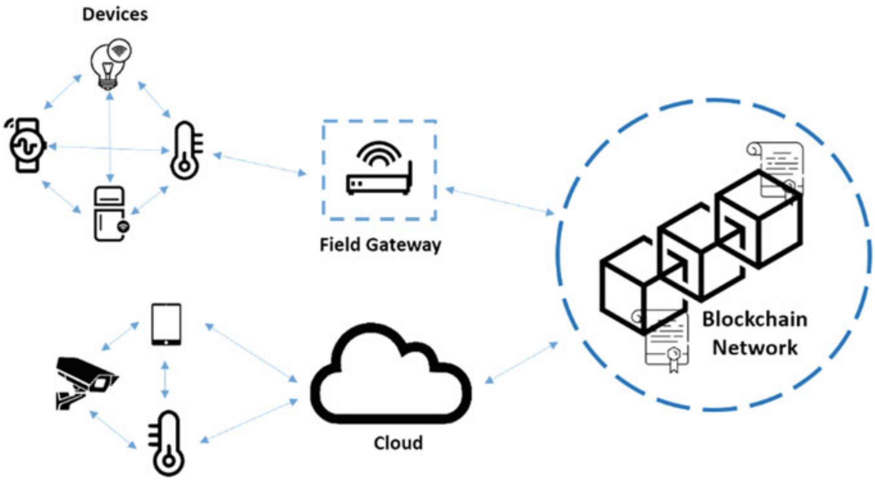


Fig. 11.10 Hybrid approach

action and even cloud computing to complement Blockchain and IoT limitations. For example, fog computing requires fewer computational connection devices such as gateways. It is a possible place where mining can take place in the same way as other initiatives that use IoT devices.

This approach expands the previous integration design, whereby IoT users decide to use the Blockchain for certain IoT interaction events, and the rest of the transactions transpire directly between IoT devices (Khan and Salah 2018). This approach leverages the benefits of decentralized record-keeping through Blockchains as well as real-time IoT delivery. Figure 11.10 is a representation of this hybrid integration approach. However, this approach optimizes the portion between the interactions that occur in real-time and those that go through the Blockchain. This allows critical core functions, compute, communicate, control, storage and decision making to be more accurate. This approach is very beneficial for areas where data latency, privacy and other data intensive issues are creating cost.

11.4.5 Advantages of Integration of IoT and Blockchain

In a centralized architecture, there are issues related to bottlenecks and central points of failure. Moving to a Blockchain architecture will solve this issue (Minoli and Occhiogrosso 2018). Since the storage area becomes decentralized, more modest companies can regulate the data and process them to a centralized architecture where large companies control it. Besides, it also enables better fault tolerance and scalability in the system. The identification of the connected devices is necessary since this points to security and trust issues. By employing a single Blockchain system, connected devices can be identified as a unique entity. The identity is also important for classification the owner device of data generated. Besides, the Blockchain also stores authentication of the IoT devices. The smart devices will be able to interact even in the absence of servers. The IoT can apply this for differentiating applications. The system is also reliable since there is no data loss range through the Blockchain (Dastjerdi and Buyya 2016). The users will confirm the data legitimacy to ensure that the data is still unimpaired without any change. The system will also allow to trace and account for the data. Therefore, authenticity is the main factor for considering the integration.

The data stored in the Blockchain as a transaction which makes it more security a resistant to alter. It can be exchanged in the form of transactions which is verified by smart contracts. Secure principles may be deployed to safely embed the codes in the IoT devices. This can enable the companies to trace the devices and update them confidentially (Sharma et al. 2017). The integration can also create an atmosphere for use in markets, where the transactions between different players can be performed without any authorities; micropayments can be done directly even when there is no trust between different people. This can develop the IoT working principle by granting more data into the Blockchain. When Blockchains are combined, it has to be seen whether the devices within the system can interact with each other. A new layer is included between the IoT devices and cloud computing for better assimilation in fog computing.

11.5 Challenges of Integration of IoT and Blockchain

The Internet of Things (IoT), is defined as a system wherein millions of physical objects or devices from around the world are connected through the Internet to share and collect data. This has been possible due to the launch of super-cheap computer chips and the presence of wireless networks all over the world. Presence of such technology it is now possible to turn anything, from as small as a needle to something as huge as an aero plane, into a part of IoT. The connection of all these devices with each other and the addition of sensors to them adds a level of digital intelligence to the devices. Such connection helps in the transmission of data wirelessly that too without the involvement of human beings. The Internet of Things has now made the world smarter and more efficient by connecting the digital world with the physical world.

The evolution of Blockchain technology was a remedy to deal with the problems that IoT technology possessed. The technology managed to eradicate the privacy and security concerns but the technology itself has a set of problems thus creating a new issue. Blockchain technology has problems namely, the ledger storage facility, limited development in technology, lack of skilled workforce, lack of proper legal codes and standards, variations in processing speeds and time, computing capabilities and some scalability issues (Khan et al. 2021). All these issues aroused when Blockchain technology and IoT technology were clubbed together. Blockchain technology was introduced as an attempt to overcome the privacy and reliability concerns of IoT. But as mentioned above the Blockchain technology also has its own sets of limitations thus, making it a bigger challenge to deal with. So, when both the technologies are integrated it causes a problem. All the challenges that come are mentioned above. To overcome this, one has to understand each of the challenges and the problems that it creates.

11.6 IoT-Based Blockchain Applications

To meet the challenges posed by IoT, the technology was integrated with another technology named Blockchain technology. The IoT technology had the problem of privacy and security of data. Many industries like the health industry, music industry, supply chain industry, business and many more are the ones currently using IoT technology. But due to its limitation on grounds of privacy and security, it was integrated with Blockchain technology. The integration did lead to solving problems that previously the industry was facing. Thus, the maximum number of sectors today have integrated both the technology to use it for their day-to-day transactions. Below we will look for areas where both IoT and Blockchain technology are used:

11.6.1 Healthcare Industry

The healthcare industry is one such industry that uses technology in its day-to-day activities. The industry is known to the biggest user of both the technology. The industry has realized that if both the IoT technology and Blockchain technology are integrated it can yield lucrative results to the entire health care sector. The FDA has made it mandatory to possess a unique device identification (UDI) code for all kinds of medical devices. Smart codes can be created by including RFID sensors embedded in the barcode labels. The reason behind using RFID is that it can be used by the hospital for keeping a track of the medical assets. The entire medical industry is looking for a solution that uses a global RFID network for the identification of medical assets. Currently, several hospitals are using RFID and barcodes with an IoT device and Blockchain technology.

11.6.2 Supply Chain Management

The shipping industry has not been receptive to adopting digital technologies, including web-based processing of information (Mollah et al. 2021). This is because there exist several kinds of barriers like the industry has to have multiple regulatory clearances when goods move across the borders. All these clearances require a lot of paperwork and their cost amounts to about 15–50% of the total shipping costs. If the global supply chain is optimized the industry can get numerous benefits from it like inventor management will be more effective, one can be more accurate when it comes to calculating cargo lead time and orders can be fulfilled more quickly. The advantages of using Blockchain technology have offered significant momentum to the digital transformation of the shipping industry. Handling the contracts is still a task that is done by humans in the industry and thus is prone to errors. If this process is done with the help of some technology, management of the contracts will be more effective and efficient as information will directly be entered into the forms as and when the cargo moves through multiple custom clearing areas (Atlam and Wills 2020). Adoption of Blockchain technology in this process will lead to a more secure documentation system. During the process of shipment, it is very imperative to know about the status of shipment and the condition of the cargo that is being shipped. Using IoT devices, like for instance temperature sensors within the shipping containers and installation of cameras will offer an audit trail that shall prove that the contents were handled carefully during the shipment process. The IoT devices will also produce data at regular intervals which can be included in the required Blockchain.

11.6.3 Smart Energy Grids

People today have become very much aware of the environment. Not only the people but the government of almost all countries have understood the value of protecting the environment. They have started considering green and renewable energy resources like biofuels, hydroelectric, solar energy, etc. Instead of the resources that were being used for a very long period. The government of California has also come up with policies including tax rebates, solar panel installation to encourage its citizens to adopt measures that help generate electricity through solar panel. But despite the installation being done by the citizens, they fail to enjoy the monetary benefits offered by the government in terms of the price per kilowatt-hour as it is governed by free-market principles. This is because the energy generated through solar panels fails to be recorded in the meters installed at people's households. So, several studies were done that suggested that the use of IoT devices can help in recording the units of energy produced through solar panels into the meters. There are different kinds of smart meters available (Minoli and Occhiogrosso 2018) like smart meters with in-home displays and meters with demand control. These can help tackle all the limitations which arise in the metering process.

11.7 Smart Home Security

Smart home refers to a house that is more automated devices are monitoring and controlling home attributes such as temperature, lighting and appliance (S. Suresh and P. V. Sruthi). The Internet of Things (IoT) facilitated to make our home more automated, regular devices such as air conditioner, refrigerator and even door locker are now able to send and receive data through the Internet. The IoT industry is growing fast; as cheaper IoT devices come every day, they transformed our homes by making them smarter and more efficient (Hwang and Hoey 2012). Various home devices such as lights, TVs and Refrigerators are now more automated and intelligent. These devices can communicate themselves without human intervention.

Intelligent devices are meant to make our lives easier. A smart fridge that monitors groceries are running out can be very convenient, but they are also gathering our private data. IoT is all about smart, but how secure these devices are will determine whether we should continue using these devices in our homes or not (Fig. 11.11).

The data collected and transmitted is mainly invisible to ordinary users. The same goes for the software built into their devices. Therefore, who has access to the data

Fig. 11.11 Connected home presentation

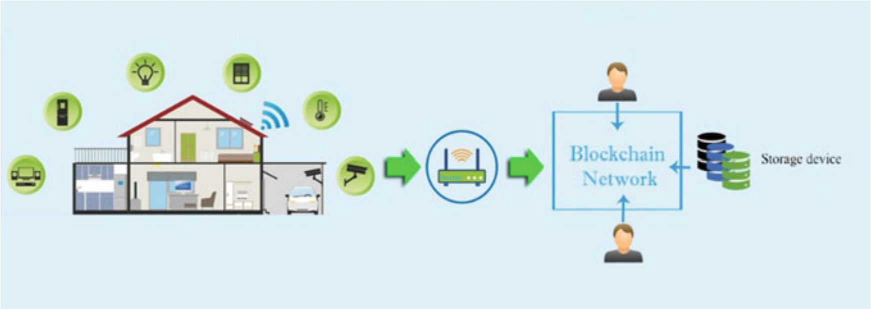


Fig. 11.12 Blockchain-based smart home

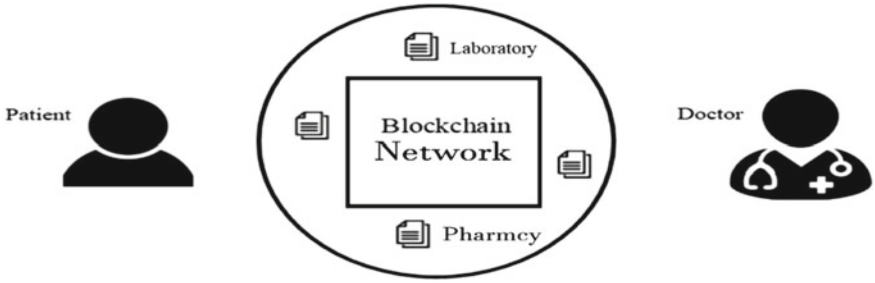


Fig. 11.13 Blockchain-based healthcare

collected and, in the worst case, who can remotely control the smart devices are the most prominent concerns in these smart home devices we keep in our house.

Not all IoT devices have meager security or commonly known credentials such as "Password as a Password." but overall, these devices come with low computing power and address privacy and concerns. Hacking smart home devices is a significant concern, but the worst case is using these devices to attack running services.

11.7.1 Typical Smart Home Security Tips

Suggestions about securing smart home devices come every day after a successful attempt to hack them (Alladi et al. 2020). Many security experts usually try to attack these IoT devices to improve their security, but hackers always find another way to cross those lines. There are several tips suggested by the manufacturers or researchers on this topic to help secure smart homes. The following are some common tips to secure smart home:

i. *Router Firmware Update*

   Router manufacturers release these firmware updates that are usually patching vulnerabilities. Therefore, it is good practice to keep the router firmware update.

ii. *Password*

   The router itself, to which all the devices are connected, should have a strong password. Most routers come with weak or guessable password; therefore, consider changing the password immediately after the purchase. In most cases, these devices are compromised due to the lousy password it comes with.

iii. *Separate Network for Smart Devices*

   Use a separate network for the Internet of Things or smart home accessories. Segmenting all the smart home device on a different network then the main devices such as laptop, desktop, tablet or cell phone. These devices should have a higher computing power and they might not be as vulnerable as IoT devices in the home.

11.7.2 Smart Home Security Solution with Blockchain

There are a lot of proactive solutions to secure smart home devices from being attacked, but they often come after a successful malicious cipher crime attempt. However, after some time, we see even those proactive solutions outsmarted by some malicious attackers (Fig. 11.12).

Blockchain addresses these issues and offers a decentralized alternative to set up smart home devices (Bedi et al. 2021). This allows users to control and authorize access to their smart homes in a fully P2P fashion. Homeowners can securely authorize access to their smart homes. Authorized ones can seamlessly control lights, thermostats and other connected devices and can even unlock "add-on" rooms or equipment closets in real-time through a convenient mobile application. With Blockchain, homeowners can enjoy full control of their smart homes and data while having the very secure formation of controlling home accessories and accessing the data. To bring it full circle, access can be securely shared with multiple people, and all terms between parties are enforce by smart contracts.

11.8 Blockchain for Healthcare Industry

The main challenge facing the healthcare industry today is the issue of security on electronic healthcare records (“Healthcare Cyber-attacks” 2019). The healthcare information record is very confidential as it contains very private and sensitive data (Nwosu et al. 2021). The emergence of the Internet of medical things (IoMT) has brought considerable vulnerability and privacy issues to the healthcare industry. These small devices track real-time healthcare conditions and even takes suitable action without human intervention (Coetzee and Eksteen 2011). On examining the safety and protection requirements of electronic healthcare records, there is an urgent necessity for a Blockchain-relied technology known as Hyperledger fabric to boost the security and privacy of the medical healthcare system (Egala et al. 2021) so that an efficient control mechanism on medical record management will be achieved. Figure 11.13 demonstrates how Blockchain can be utilized to secure patient’s data.

There is a particular opportunity for the Blockchain revolution to disrupt and lead a digital transformation. With the use of Blockchain in the pharmaceutical supply chain, the potential supply chain grows exponentially (Nwosu et al. 2021). With the help of Blockchain, every point of the pharmaceutical supply chain can be recorded to one of the blocks belonging to the Blockchain (Longo et al. 2019). The newest copies on the entire ledger will be distributed to a higher number of computers, making the information highly available and transparent (Fig. 11.14).

Building trust in the healthcare supply chain is another benefit of using the Blockchain as any block connected to the previous one. Thus, it is extremely difficult to compromise the security of the Blockchain. As the medication condition before it reaches the medical centers is crucial, it is essential for healthcare providers to

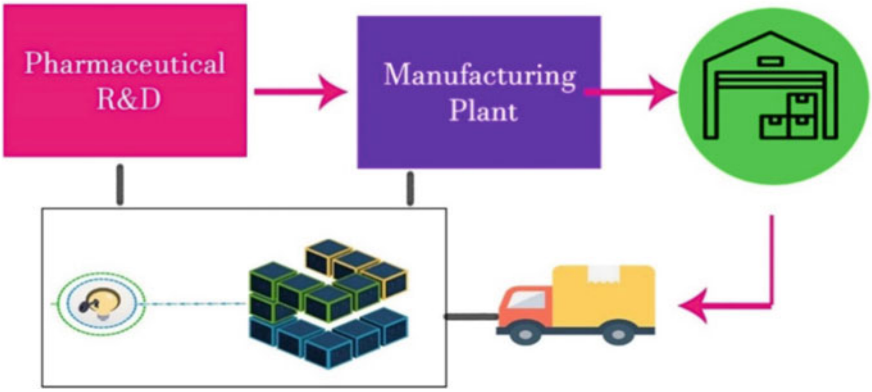


Fig. 11.14 Applied blockchain to medical supply chain

follow the medications from the source until it reaches the target patient. The above Figure # illustrates medical supply chain-based Blockchain technology.

11.9 Results

Overall, the results presented below show that; by taking Blockchain concepts and apply them to the IoT, the possibility of hacker infecting the system will be nearly impossible (Dai et al. 2019). Blockchain extends a scalable and decentralized environment to IoT devices, platforms and applications. Delivering integrity has always been a significant challenge in the IoT ecosystem. On the contrary, Blockchain drives integrity around the data and enhances the management of IoT networks. We have also shown a substantial number of opportunities where if we enable Blockchain in the IoT space, we provide an end-to-end secure business opportunity.

In the following table (Table 11.4) we have shown a few Blockchain Enterprise use cases on how combining IoT with Blockchain can have a significant impact across multiple industries:

Identity credentials for an IoT device and data can be registered as a transaction record in a Blockchain block. Unauthorized operations of stored IoT data can be detected, making the system compact and resistant to temper. Data can be safely stored in the Blockchain nodes; no central authority, such as a cloud storage provider, is needed to protect IoT data. Blockchain uses superior data encryption algorithms for more security and privacy application. This application is primarily performed for financial services for more risk freedom. IoT devices may send and receive information in the same way as financial transactions, and integrating with Blockchain enables secure data communication between connected things (Table 11.5).

Internet of Vehicles (IoV) is the innovation of that conventional vehicular ad hoc network (VANET), which refers to the network of different entities, such

Table 11.4 IoT-based blockchain for enterprise use cases

S No.	Use case	IoT–based blokchain solution
1	Supply chain and logistics	Companies are operating on making the vehicles IoT-enabled to track the journey throughout the shipment process. Owing to the lack of transparency and complications in the current supply chain and logistics, Blockchain and IoT integration can enhance the network's reliability and traceability by storing the information transparently and tamperproof
2	Automotive industry	Automotive industries are now using IoT-enabled sensors to operate more efficiently. Connecting IoT-enabled vehicles with the decentralized network enables various users to exchange crucial information efficiently and quickly. IoT-based Blockchain can help secure and reliable transactions for automated fuel payment, smart parking and automated traffic control
3	Smart homes	Smart IoT-enabled devices take part in our everyday lives. Smartphones enable applications that are used to control IoT devices, and with Blockchain integrated, the security of home devices will be concrete. But the traditional centralized method to exchange information generated by IoT devices go without security standards and ownership of data. Blockchain could advance the smart home to the next level by solving security issues and removing centralized infrastructure
4	Sharing economy	Sharing economy has become a widely adopted abstraction around the globe. Blockchain could build decentralized, shared economy applications to receive considerable revenue by sharing the goods seamlessly
5	Pharmacy industry	Feigned medicine in the pharmaceutical sector is rising every day. The pharmacy industry is accountable for developing medications, manufacturing drugs and distributing drugs. Therefore, tracking drugs' complete journey is very hard. Blockchain technology's transparency and traceable nature can help monitor drugs' shipment from their origin to the supply chain destination

as city infrastructure, vehicles, pedestrians, roads, parking and lots and provides real-time communication among them. The decentralization, heterogeneity and non-trustworthiness of IoV reveal challenges in securing communications and transaction-execution. Integrating Blockchain with IoV can address the above challenges. Moreover, Blockchain technologies can be used to protect both the energy and information interactions between electric vehicles among other industries (Table 11.6).

Core working capabilities of Blockchain enable a duly decentralized, trusted ledger of all network transactions. This capability can allow the assents and regulatory requirements for IoT systems (Zhang and Wen 2017). Although there are many appealing benefits of adopting Blockchain for IoT security and privacy challenges,

Table 11.5 IoT challenges addressed by blockchain

S No.	IoT challenge	Blockchain-based IoT solutions
1	Security	Data is recorded in chronological order on a continuously growing database. Any malicious activity can be easily determined and resolved because data verified before storing
2	Privacy	Digital signatures and cryptography are applied to secure the data transfer
3	Device Identity	Blockchain gives each device a unique encrypted identity
4	Man, in the middle attack	Blockchain facilitates peer-to-peer data transfer without a central intermediary. Even if one of the network security devices is being compromised, the attacker will not see the data or manipulate it

Table 11.6 Applications of blockchain of things and benefits

S No.	Application	Benefits	References
1	IoV and UAVs	• Ensure security, safety and transparency • Reduce the impact of malicious nodes efficiently • Guaranteeing mutual-confidence among UAVs	
2	Health care	• Robust security • Safeguard privacy • Verifying authenticity • Trustworthiness information	(Ray et al. 2021)
3	Smart grid	• Secure energy operation • Improve transparency • Preserving privacy	(Zhuang et al. 2021)
4	Food industry	• Improve reliability of data • Enhance traceability • better food safety	(Tse et al. 2017)
5	Supply chain management	• Transparent and anticounterfeit information • Attenuate the supply chain risk	(Konstantinidis et al. 2018)
6	Smart manufacturing	• Illuminate cost for trusted third party • Improve interoperability • Automating P2P business operation	(Christidis and Devetsikiotis 2016)

the technology is way below the perfect state because IoT implies control over a network of devices, where multi-layered security must be put in place. One of the significant obstructions to adoption is paradoxically linked to one of the stated advantages of Blockchain. Every activity on the network has to be recognized by other network participants for it to go active. For example, in case of an apparent security breach through one of the connected devices, revoking that device's entrance would significantly decrease the negative result of spreading the malware. On a grander scale, with thousands of IoT devices connected to an extensive network, it can be challenging to receive consent from the majority of entities.

11.10 Discussion

Securing IoT devices and networks is a complex puzzle expecting a comprehensive approach and inventive solutions. One possible way of improving security and reliability within an IoT ecosystem is integrating with Blockchain technology (Dorri et al. 2017). Blockchain in IoT can be the answer to two significant challenges in IoT "security and privacy". Further, Blockchain embraces the most robust encryption standards, which adds a much-needed layer of IoT stack security. Any malicious, corrupt, and critical entity/actor will bypass this superior layer to access IoT data or IoT devices, making cyber-attacks way more difficult and time-consuming of possible (Dorri et al. 2017).

As the results indicate, there is no perfect way to combine IoT with Blockchain to suit all operations. The study proposed four different approaches, which can be categorized to accommodate various use cases. For example, sensors in valves of petroleum refinery detect dangerously high pressure in the pipes, shutoffs must be triggered as soon as possible. The automatic shutoff instructions may come too late with analysis of that pressure data taking place at disturbed data management because all other network participants should validate data. A well-designed centralized system with processing power placed local to the end devices will perform better because latency is less, and that complexity and time-consuming validation can be significantly reduced. However, Blockchain security features can be utilized partially (see Chap. 4: Sect. 4.1) or integrated with cloud and edge computing creating a hybrid system to solve various latency issues in IoT with Blockchain.

On the other hand, fully decentralized Blockchain-based IoT where every transaction is directly recorded in the Blockchain could be applicable in tracking assets. Immutable records and reliable data chain are some issues that face in supply chains today. Medical products and perishable goods need to be transported across locations under strictly regulated temperature ranges and within specific time windows. Blockchain and IoT allow all partners and things in a supply chain ecosystem to share data securely.

11.11 Conclusion

This study provided a systematic survey of IoT security landscape with a specific focus on Blockchain integration to fulfill all particular requirements for secure IoT deployment. We stated that IoT devices and networks' security are complex problems requiring a comprehensive framework and creative solutions. Many IoT devices are being built with static credentials, username and password, symmetric tokens; however, all those security features are no longer sufficient. Blockchain achieved immutable and secure records through distributed consensus algorithms; therefore, we have identified the key points where Blockchain technology can improve IoT applications. By decentralizing IoT systems with Blockchain and eliminating single points of failure, connected devices receive additional security layer and become less vulnerable to malware and other attacks. It highly anticipated that Blockchain would revolutionize the IoT ecosystem. Combining these two technologies should be addressed, considering the challenges identified in this paper. The rapid increase of IoT implementation raised the scalability and storage capacity issues, which affect both technologies; Blockchain can be further used, particularly in encrypted currencies, where it will significantly increase the Internet of Things and Blockchain's compatibility. We believe that the continued integration of Blockchains in the IoT ecosystem will induce considerable evolution across several industries, bringing about new business models and having us reconsider how current systems and processes are implemented.

Security is still the common challenging issue for all new technologies that takes researchers and organizations' attention. Combining Blockchain with IoT can improve security as it uses most participants' consent to validate transactions to prevent spoofing and fraud. However, IoT devices have weak computational resources and storage space that cannot process cryptographic algorithms. Blockchain can be further explored to unite with IoT for providing better security and privacy in different innovative application domains like healthcare, logistics and manufacturing. Moreover, there will be a requirement to promote a comprehensive trust foundation or framework that meets all Blockchain requirements in IoT Blockchain systems.

We are fully confident based on our analysis, research study and results that our proposed integration mechanism of IoT and Blockchain, it will enhance the security of the data as well as the entire system.

Definitely, this work will open the new dimension to address real-issues of industries like supply chain management, health sector, smart home, smart agriculture, logistics, manufacturing, food chain systems to track the exact position of items/components and their life sustainability, reliability and removal or minimize the third party involvement from the system over and above of security on the top priority.

References

Alam S, Siddiqui ST, Ahmad A, Ahmad R, Shuaib M (2020) Internet of Things (IoT) Enabling Technologies, Requirements, And Security Challenges. In: Kolhe M, Tiwari S, Trivedi M, Mishra . (eds) Advances in data and information sciences. Lecture notes in networks and systems, vol 94. Springer, Singapore. https://doi.org/10.1007/978-981-15-0694-9_12

Alam Khan F, Asif M., Ahmad A, Alharbi M, Aljuaid H (2020) Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustain Cities Soc 55:102018. https://doi.org/10.1016/j.scs.2020.102018

Alladi T, Chamola V, Sikdar B, Choo KR (2020) Consumer IoT: security vulnerability case studies and solutions. IEEE Consum Electron Mag 9(2):17–25

Amin R, Kumar N, Biswas G, Iqbal R, Chang V (2018) A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment. Futur Gener Comput Syst 78:1005–1019. https://doi.org/10.1016/j.future.2016.12.028

Andriati A (2020) Hashing algorithms, optimized mappings and massive parallelization of multiconfigurational methods for bosons. ArXiv.Org. https://arxiv.org/abs/2005.13679

Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y et al (2018) Hyperledger fabric: a distributed operating system for permissioned Blockchains, 2018, arXiv preprint arXiv:1801.10228

Asad M, Memon AZQTJ, Alshboul R (2017) Addressing the future data management challenges in IoT: a proposed framework. Int J Adv Compu Sci Appl 8(5):198–200. https://doi.org/10.14569/ijacsa.2017.080525

Atlam H, Wills G (2020) IoT security, privacy, safety and ethics. In: Farsi M, Daneshkhah A, Hosseinian-Far A, Jahankhani H (eds) Digital twin technologies and smart cities. Springer International Publishing, Switzerland, pp 1–27

Babu B, Srikanth K, Ramanjaneyulu T, Narayana I (2016) IoT for healthcare. Int J Sci Res (IJSR) 5(2):322–326. https://doi.org/10.21275/v5i2.nov161096

Bach LM, Mihaljevic B, Zagar M (2018) Comparative analysis of blockchain consensus algorithms. In: 2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO), Opatija, Croatia, pp 1545–1550. https://doi.org/10.23919/MIPRO.2018.8400278

Bedi P, Goyal SB, Kumar J, Kumar S (2021) Blockchain integrated framework for resolving privacy issues in smart city. In: Chakraborty C, Lin JCW, Alazab M (eds) Data-driven mining, learning and analytics for secured smart cities. Advanced sciences and technologies for security applications. Springer, Cham. https://doi.org/10.1007/978-3-030-72139-8_6

Bekerman D, S Y, Lowing S, Klepfish N, Hasson E, Lynch B, McKeever G (2020) The state of vulnerabilities in 2019 | Imperva. Blog. Geraadpleegd op 17 april 2022, van https://www.imperva.com/blog/the-state-of-vulnerabilities-in-2019/

Brachmann M, Keoh SL, Morchon OG, Kumar SS (2012) End-to-end transport security in the IP-based Internet of Things. In: 2012 21st international conference on computer communications and networks, ICCCN. pp 1–5. http://dx.doi.org/10.1109/ICCCN.2012.6289292

C K (2018) An overview of blockchain technology. Int Res J Electron Comput Eng 4(4):1. https://doi.org/10.24178/irjece.2018.4.4.01

Ch R, Srivastava G, Reddy Gadekallu T, Maddikunta PKR, Bhattacharya S (2020) Security and privacy of UAV data using blockchain technology. J Inf Secur Appl 55:102670 https://doi.org/10.1016/j.jisa.2020.102670

Chen C-H, Lin Y-A, Wu W-T, Huang Y-T, Chu C-C (2019) Design and implementation of IPv4 and IPv6 provisioning technologies for VPC architecture. In: 2019 20th Asia-Pacific network operations and management symposium (APNOMS) Sep 2019, pp 1–4, https://doi.org/10.23919/APNOMS.2019.8892911

Chioma BF (2020) Internet of things (IoT): A review of enabling technologies, challenges and open research issues. Int J Res Appl Sci Eng Technol 8(4):277–285. https://doi.org/10.22214/ijraset.2020.4044

Chow SS, Choo KKR, Han J (2021) Editorial for accountability and privacy issues in Blockchain and cryptocurrency. Futur Gener Comput Syst 114:647–648. https://doi.org/10.1016/j.future.2020.08.039

Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the Internet of Things. IEEE Access 4:2292–2303

Coetzee L, Eksteen J (2011) The internet of things—promise for the future? An introduction. IST-Africa Conf Proc 2011:1–9

Dai H-N, Zheng Z, Zhang Y (2019) Blockchain for internet of things: a survey. IEEE Internet Things J 6(5):8076–8094. https://doi.org/10.1109/JIOT.2019.2920987

Damara AR, Indriani OR, Sari CA, Setiadi DRIM, Rachmawanto EH (2017) Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5). In: 2017 international conference on smart cities, automation & intelligent computing systems (ICON-SONICS), Yogyakarta, Indonesia, pp 87–92, https://doi.org/10.1109/ICON-SONICS.2017.8267827

Dastjerdi AV, Buyya R (2016) Fog computing: helping the internet of things realize its potential. Computer 49(8):112–116. https://doi.org/10.1109/mc.2016.245

De Silva S, Goyal SB, Bedi P (2021) Security challenges of digital currency system. In: Abraham A, Sasaki H, Rios R, Gandhi N, Singh U, Ma K (eds) Innovations in bio-inspired computing and applications. IBICA 2020. Advances in intelligent systems and computing, vol. 1372. Springer, Cham. https://doi.org/10.1007/978-3-030-73603-3_51

Dixon P (2017) A failure to "Do No Harm"—India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. Health and Technology 7(4):539–567. https://doi.org/10.1007/s12553-017-0202-6

Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: Proceeding of the IEEE International Conferences Pervasive Computing andCommunications. Workshops (PerCom Workshops), pp 618–623

Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J 8(14):11717–11731, 15 July 2021

Eris Industries Documentation—Blockchains. Accessed on 15 Mar 2016. [Online]. Available: https://docs.erisindustries.com/explainers/Blockchains/

Foti M, Mavromatis C, Vavalis M (2021) Decentralized Blockchain-based consensus for optimal power flow solutions. Appl Energy 283:116100. https://doi.org/10.1016/j.apenergy.2020.116100

Golosova J, Romanovs A (2018) The advantages and disadvantages of the blockchain technology. In: 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE). Vilnius, Lithuania, pp 1–6, https://doi.org/10.1109/AIEEE.2018.8592253

Granjal J (2014) Network layer security for the Internet of Things using TinyOS and BLIP. Wiley Online Library. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.2444

Hang L, Kim D-H (2019) Design and implementation of an integrated IoT Blockchain platform for sensing data integrity. Sensors 19(10):2228. https://doi.org/10.3390/s19102228

Healthcare Cyber Attacks (2019) J Vascular Nurs 37(4):225. https://doi.org/10.1016/j.jvn.2019.12.001

Hendricks D (2015) The trouble with the internet of things. London Datastore. Greater London Authority. Retrieved 10 Aug 2015

Hwang A, Hoey J (2012) Smart Home the next generation: closing the gap between users and technology. In: AAAI Technical Report FS-12–01 AI for Gerontechnology AAAI Fall Symposium

Ishmaev G (2020) Sovereignty, privacy, and ethics in Blockchain-based identity management systems. Ethics Inf Technol. https://doi.org/10.1007/s10676-020-09563-x

Janssen M, Weerakkody V, Ismagilova E, Sivarajah U, Irani Z (2020) A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors. Int J Inf Manage 50:302–309. https://doi.org/10.1016/j.ijinfomgt.2019.08.012

Khan Y, Goyal SB, Bedi P (2021) Security challenges of blockchain. In: Abraham A, Sasaki H, Rios R, Gandhi N, Singh U, Ma K (eds) Innovations in bio-inspired computing and applications. IBICA 2020. Advances in intelligent systems and computing, vol. 1372. Springer, Cham. https://doi.org/10.1007/978-3-030-73603-3_23

Khan MA, Salah K (2018) IoT security: review blockchain solutions, and open challenges. Future Gener. Comput. Syst. 82:395–411

Khettry AR, Patil KR, Basavaraju AC (2021) A Detailed review on blockchain and its applications. SN Comput Sci 2(1):5–9. https://doi.org/10.1007/s42979-020-00366-x

Khor JH, Sidorov M, Woon PY (2021) Public blockchains for resource-constrained IoT Devices -A state of the art survey. IEEE Internet of Things J 1. https://doi.org/10.1109/jiot.2021.3069120

Kim H, Lee H, Lee Y (2020) A survey analysis of internet of things security issues and combined service 25(8):73–79. https://doi.org/10.9708/JKSCI.2020.25.08.073

Komargodski I, Segev G (2020) From minicrypt to obfustopia via private-key functional encryption. J Cryptol 33:406–458. https://doi.org/10.1007/s00145-019-09327-x

Konstantinidis I, Siaminos G, Timplalexis C, Zervas P, Peristeras V, Decker S (2018) Blockchain for business applications: a systematic literature review. In: Abramowicz W, Paschke A (eds) Business information systems. Springer International Publishing, Cham, pp 384–399

Lansiti M, Lakhani K (2017) The truth about blockchain. Harvard Bus Rev. [online] Available: https://hbr.org/2017/01/the-truth-about-Blockchain

Longo F, Nicoletti L, Padovano A, d'Atri G, Forte M (2019) Blockchain-enabled supply chain: an experimental study. Comput Ind Eng 136:57–69. https://doi.org/10.1016/j.cie.2019.07.026

Mahda MN, Mohammed A, Gaedke M (2017) Interoperability in Internet of Things infrastructure: classification, challenges, and future work (In Press)

Micro T (2018) Backdoor attacks: How they work and how to protect against them. Trend Micro, Inc. https://blog.trendmicro.com/backdoor-attacks-work-protect

Minoli D, Occhiogrosso B (2018) Blockchain mechanisms for IoT security. Internet of Things 1–2:1–13. https://doi.org/10.1016/j.iot.2018.05.002

Miraz MH, Ali M (2018) Applications of blockchain technology beyond cryptocurrency. Ann Emerg Technol Comput 2(1):1–6. https://doi.org/10.33166/aetic.2018.01.001

Mollah MB et al (2021) Blockchain for future smart grid: a comprehensive survey. IEEE Internet Things J 8(1):18–43, 1 Jan 2021, https://doi.org/10.1109/JIOT.2020.2993601

Noura M, Atiquzzaman M, Gaedke M (2019) Interoperability in internet of things: taxonomies and open challenges. Mobile NetwAppl 24:796–809. https://doi.org/10.1007/s11036-018-1089-9

Nwosu AU, Goyal SB, Bedi P (2021) Blockchain transforming cyber-attacks: healthcare industry. In: Abraham A, Sasaki H, Rios R, Gandhi N, Singh U, Ma K (eds) Innovations in bio-inspired computing and applications. IBICA 2020. Advances in intelligent systems and computing, vol. 1372. Springer, Cham. https://doi.org/10.1007/978-3-030-73603-3_24

Othman MM, El-Mousa A (2020) Internet of things & cloud computing internet of things as a service approach. In: 2020 11th international conference on information and communication systems (ICICS). Irbid, Jordan, pp 318–323, https://doi.org/10.1109/ICICS49469.2020.239503

Porambage P, Ylianttila M, Schmitt C, Kumar P, Gurtov A, Vasilakos AV (2016) The quest for privacy in the internet of things. IEEE Cloud Comput 3(2):36–45, Mar-Apr 2016, https://doi.org/10.1109/MCC.2016.28

Ray PP, Dash D, Salah K, Kumar N (2021) Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Syst J 15(1):85–94. https://doi.org/10.1109/JSYST.2020.2963840

Raza S, Voigt T, Jutvik V (2012) Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security. In: Proceedings of the IETF workshop on smart object security, vol. 23

Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and its integration with IoT. Challenges and opportunities. Future Gener Comp Sys 88:173–190. https://doi.org/10.1016/j.future.2018.05.046

Rios VDM, Inácio PR, Magoni D, Freire MM (2021) Detection of reduction-of-quality DDoS attacks using fuzzy logic and machine learning algorithms. Comput Networks 186:107792. https://doi.org/10.1016/j.comnet.2020.107792

Rouse M (2019) Internet of things (IoT). IOT Agenda. Retrieved 14 Aug 2019

Sestino A, Prete MI, Piper L, Guido G (2020) Internet of Things and big data as enablers for business digitalization strategies. Technovation 98:102173. https://doi.org/10.1016/j.technovation.2020.102173

Shahid F, Khan A (2020) Smart digital signatures (SDS): a post-quantum digital signature scheme for distributed ledgers. Futur Gener Comput Syst 111:241–253. https://doi.org/10.1016/j.future.2020.04.042

Sharma PK, Singh S, Jeong Y-S, Park JH (2017) Distblocknet: a distributed Blockchains-based secure sdn architecture for iot networks. IEEE Commun Mag 55(9):78–85

Sinha S, Pradhan C (2021) Blockchain technology enabled digital identity management in smart cities. In: Tamane SC, Dey N, Hassanien AE (eds) Security and privacy applications for smart city development. Studies in systems, decision and control, vol 308. Springer, Cham. https://doi.org/10.1007/978-3-030-53149-2_7

Statista (2021) Internet of things—number of connected devices worldwide 2015–2025. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Tse D, Zhang B, Yang Y, Cheng C, Mu H (2017) Blockchain application in food supply information security. In: 2017 IEEE international conference on industrial engineering and engineering management (IEEM), Dec 2017, pp 1357–1361

Tseng L, Wong L, Otoum S, Aloqaily M, Othman JB (2020) Blockchain for managing heterogeneous internet of things: a perspective architecture. IEEE Netw 34(1):16–23. https://doi.org/10.1109/MNET.001.1900103

Weber RH (2010) Internet of things—New security and privacy challenges. Comput Law Secur Rev 26(1):23–30. https://doi.org/10.1016/j.clsr.2009.11.008

Yánez W, Mahmud R, Bahsoon R, Zhang Y, Buyya R (2020) Data allocation mechanism for internet-of-things systems with blockchain. IEEE Internet Things J 7(4):3509–3522. https://doi.org/10.1109/JIOT.2020.2972776

Yang R, Wakefield R, Lyu S, Jayasuriya S, Han F, Yi X, Yang X, Amarasinghe G, Chen S (2020) Public and private Blockchain in construction business process and information integration. Autom Constr 118:103276. https://doi.org/10.1016/j.autcon.2020.103276

Yeow K, Gani A, Ahmad RW, Rodrigues JJ, Ko K (2018) Decentralized consensus for edge-centric internet of things: a review, taxonomy, and research issues. IEEE Access 6:1513–1524

Zhang K, Liang X, Lu R, Shen X (2014) Sybil attacks and their defenses in the internet of things. IEEE Internet Things J 1(5):372–383. https://doi.org/10.1109/JIOT.2014.2344013

Zhang Y, Wen J (2017) The IoT electric business model: using blockchain technology for the internet of things. Peer-to-Peer Netw Appl 10:983–994. https://doi.org/10.1007/s12083-016-0456-1

Zhu X, Badr Y (2018) Identity management systems for the internet of things: a survey towards blockchain solutions. Sensors 18(12):4215. https://doi.org/10.3390/s18124215

Zhuang P, Zamir T, Liang H (2021) Blockchain for cybersecurity in smart grid: a comprehensive survey. IEEE Trans Ind Inf 17(1):3–19. https://doi.org/10.1109/TII.2020.2998479

Chapter 12
Challenges and Trends on Post-Quantum Cryptography

Kunal Das and Arindam Sadhu

12.1 Introduction

Every day trillions of data are processed in the banking sector, government offices, personnel chat in social networks, and even any online purchase, etc., through the Internet. A few days back, we noticed Domino's pizza server was hacked; all customer details were available on the dark Internet. Our phone number, email ID, and even our private information like bank details, choice, food habits, family details, and our monthly income can be analysed from these data. Every day this type of attack is happening in every network. Every day the attempt is made to attack in this Internet of Things era. Our privacy is in big question due to such attacks due to lack of security.

This chapter explores how classical cryptographic algorithms are facing challenges due to quantum algorithm advancements. Even it is not so far that quantum algorithm will be able to break the classical security. Section 12.2 describes the challenges due to the quantum algorithm for large prime number factorization, which, as we know, is an essential requirement to break any cryptographic algorithm like RSA algorithm, etc. Section 12.3 focuses on the progress of the post-quantum algorithm, which is not able to break even by quantum computers. The quantum digital cheque algorithm for online banking transactions to secure our transaction as post-quantum cryptography is explored in Sect. 12.5. Finally, we conclude the importance of this chapter in Sect. 12.6.

K. Das (✉)
Acharya Prafulla Chandra College, New Barrackpur, Kolkata, WB 700131, India
e-mail: kunal@apccollege.ac.in

A. Sadhu
Maulana Abul Kalam Azad University of Technology, Kolkata, WB, India

Greater Kolkata Engineering and Management, Baruipur, Kolkata, WB, India

S. Saxena and A. K. Pradhan (eds.), *Internet of Things*, Transactions on Computer Systems and Networks, https://doi.org/10.1007/978-981-19-1585-7_12

12.2 Challenges Due to Shor's Algorithm

Classical encryption algorithms, RSA cryptosystem, public key cryptography, and digital signature algorithm (Rosen and Krithivasan 2012) are fundamental asymmetric key encryption codes that are assumed to NP-hard problem to break or crypto analysis. However, several attack policies are reported in different research articles (Rosen and Krithivasan 2012; Saxena et al. 2017). Overall it is still considered to be secured. However, it is still secured until quantum algorithms and quantum computers with many qubits are not available in the world. For simple understanding, why do we consider RSA algorithm is secured? The answer is well known because, in general, private keys cannot decode as factorization of large numbers into two prime numbers, i.e. $n = p*q$ (p, q are large prime numbers), is not possible by classical computer and classical algorithm, requiring exponential running time. It is an NP-hard problem; classical computers may need a few years to factor in the large number. So, fundamentally we are safe and secure other than attack, etc. But the big dollar question is how long we are secure? Conventional security will face significant challenges in the post-quantum computer era. Already industries like D-wave, IBM, Honeywell, Google, and many more are successfully developed quantum computers. The algorithm that will be discussed in Sect. 1.1 is called Shor's algorithm (Rosen and Krithivasan 2012; Saxena et al. 2017), which can break RSA encryption code within linear time computation. Thereafter, a question will come to the reader why is RSA encryption still not broken? Whether answer will justify how long we are secured. Again we do not know as quantum computer still not reached that numbers of qubits. In Sect. 1.1, we explain the Shor's algorithm (Full chapter will include more in Sect. 1.2 Experimental implementation, etc.).

12.2.1 Shor's Algorithm

In this subsection, we demonstrate the power of the quantum computer to break classical cryptography or encryption code. Shor's algorithm got the attention of all researchers in the field of cryptography. It is famous to factoring integer numbers in polynomial time. Since any classical computer required exponential time to factoring large integer numbers into two prime numbers, exploit this for classical cryptosystem, RSA keeping faith on that classical computer cannot break it. But this myth is no longer going to continue as quantum computer development is progress.

In this subsection, we need to know that Shor's algorithm can factor a large integer number into two prime numbers $n = p*q$ and p, q which are large prime numbers (McMahon 2007). Shor's algorithm quantum part is to do order finding; more specifically, Shor's algorithm has two parts: the quantum and classical parts. If a classical algorithm can efficiently solve some parts like quantum, we do not need to do it quantum way. This concept is called hybrid computing.

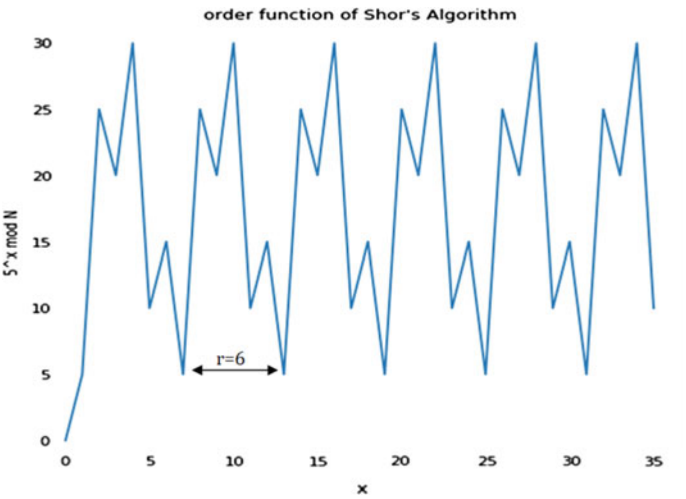


Fig. 12.1 Order function of Shor's algorithm

Now, let us know what is order finding or period finding. The order or period function $(x) = a^x \mod N$, where a and N are positive integers, a is less than N, and have no common factors. The order or period (r) is such that a^rmed $N = 1$. In Fig. 12.1, we have shown order or period function plot. In this example, we have considered $a = 5$, $N = 35$, an odd number, since N is product of two large prime numbers always being odd number. From Fig. 12.1, we can find the order or period $r = 6$.

In order to solve in the quantum algorithm the problem of order finding, we can consider it as a unitary operation. A unitary matrix represents the unitary operator, and the matrix is said to be unitary if $U{*}U^{\ddagger} = I,$ where I is the identity matrix.

$$U_x|Y\rangle = \begin{cases} |xy \mod N\rangle \; 0 \le y \le N-1 \\ |y\rangle N \le \qquad y \le 2^L - 1 \end{cases} \tag{12.1}$$

where $L = \lceil \log N \rceil$ the eigenstates U_x and eigenvalues $U_x|u_t\rangle$.

Let us now check with the same example we have considered $a = 5$, $N = 35$, and $5^r \mod 35 = 1$.

For example, $U_1|1\rangle = |5 \mod 35\rangle = 5$, $U_2|1\rangle = \left|5^2 \mod 35\right\rangle = 25$, $U_3|1\rangle = \left|5^3 \mod 35\right\rangle = 20$.

$$U_4|1\rangle = \left|5^4 \mod 35\right\rangle = 30,\ U_5|1\rangle = \left|5^5 \mod 35\right\rangle = 10,\ U_6|1\rangle = \left|5^6 \mod 35\right\rangle = 5$$

Hence, $r = 6$ the $U_1|1\rangle = U_6|1\rangle$. We will get an order or period equal to 6.

We can find the order with the specified input state and can compute the quantity $a^k \mod N$ using quantum parallelism.

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \mathrm{e}^{-\frac{i2\pi ks}{r}} \left|a^k \bmod N\right\rangle \tag{12.2}$$

$$U|u_s\rangle = \mathrm{e}^{-\frac{i2\pi s}{r}} |u_s\rangle \tag{12.3}$$

We have eigenstate for each integer $0 \leq s \leq r - 1$. All the computational basis will be cancelled out except $|1\rangle$ if the eigen states are added.

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \tag{12.4}$$

For $a = 5$, $N = 35$, and $r = 6$, we have

$$\begin{aligned}
&\frac{1}{\sqrt{6}}(|u_0\rangle = \frac{1}{\sqrt{6}}(|1\rangle + |5\rangle + |25\rangle + |20\rangle + |30\rangle + |10\rangle \ldots . \\
&\quad + |u_1\rangle = \frac{1}{\sqrt{6}}\Big(|1\rangle + \mathrm{e}^{-\frac{i2\pi}{6}}|5\rangle + \mathrm{e}^{-\frac{i4\pi}{6}}|25\rangle + \mathrm{e}^{-\frac{i6\pi}{6}}|20\rangle \\
&\quad + \mathrm{e}^{-\frac{i8\pi}{6}}|30\rangle| + \mathrm{e}^{-\frac{i10\pi}{6}}|10\rangle \ldots . \Big) + \\
&\ldots . \\
&\ldots . \\
&\quad + |u_5\rangle = \frac{1}{\sqrt{6}}\Big(|1\rangle + \mathrm{e}^{-\frac{i10\pi}{6}}|5\rangle + \mathrm{e}^{-\frac{i20\pi}{6}}|25\rangle + \mathrm{e}^{-\frac{i30\pi}{6}}|20\rangle \\
&\quad + \mathrm{e}^{-\frac{i40\pi}{6}}|30\rangle + \mathrm{e}^{-\frac{i50\pi}{6}}|10\rangle \ldots . = |1\rangle\Big)
\end{aligned} \tag{12.5}$$

A superposition of these eigenstates is computational basis state $|1\rangle$, quantum phase estimation on U on state $|1\rangle$, it results in measure phase Ø = s/r, where $0 \leq sr - 1$. Finally, we will find r from the given quantum circuit (Fig. 12.2).

The classical part of Shor's algorithm can formulate as following steps which can simply summarize as 'repeat–until' procedure (ref. from lecture note of John Watrous of University of Waterloo and book by David McMahon 'Quantum Computing Explained')[,].

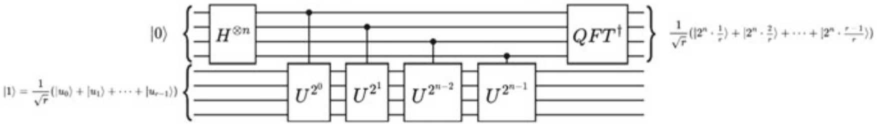

$|0\rangle$
$|1\rangle = \frac{1}{\sqrt{r}}(|u_0\rangle + |u_1\rangle + \cdots + |u_{r-1}\rangle)$
$H^{\otimes n}$
U^{2^0}
U^{2^1}
$U^{2^{n-2}}$
$U^{2^{n-1}}$
$QFT^\dagger$
$\frac{1}{\sqrt{r}}(|2^n \cdot \frac{1}{r}\rangle + |2^n \cdot \frac{2}{r}\rangle + \cdots + |2^n \cdot \frac{r-1}{r}\rangle)$

Fig. 12.2 Quantum circuit to find *r*

```
Input: Odd integer N
Repeat
    Randomly select $X \in [2, 3, \ldots, N]$ and $a \in [2, 3, \ldots N - 1]$
    $d = \gcd(X,\ N)$;
    if $d \geq 2$ then $u = d,\ v = N/d$;
    else
    Find the order or period r such that $X^r = 1 \mod N$ /* requires the order finding quantum algorithm. */
    $y = X^{r/2} - 1 \mod N$;
    $d = \gcd(y,\ N)$;
    If   if $d \geq 2$ then $u = d,\ v = N/d$;
    Until finding u, v
```

Therefore, Shor's algorithm can break classical encryption code in polynomial running time if a sufficient amount of qubits are available in quantum computers. It is becoming the prime concern of classical encryption in this Internet on Things era. The security of classical encryption has serious issues due to quantum evolutions.

12.2.2 Experimental Implementation

The order finding quantum algorithm part is implemented using IBMQ Qiskit. The classical feature is implemented using Python programming. The code we do not include in this chapter. It is available at the ref. (Farhi et al. 2012). Figure 12.1 shows the quantum gate circuit diagram to find order 'r' as a quantum part of Shor's algorithm. Figure 12.3 demonstrates the quantum circuit for order finding using IBMQ. Figure 12.4a shows the probabilities to find order 'r' for input $a = 7$ and $N = 15$ and remember last two qubits represent the order. The phase of corresponding

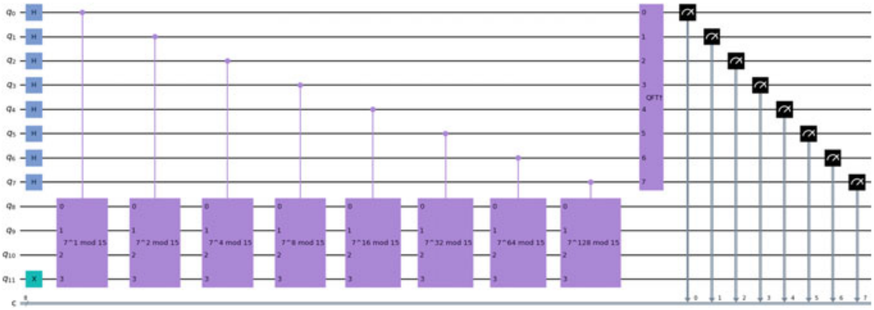
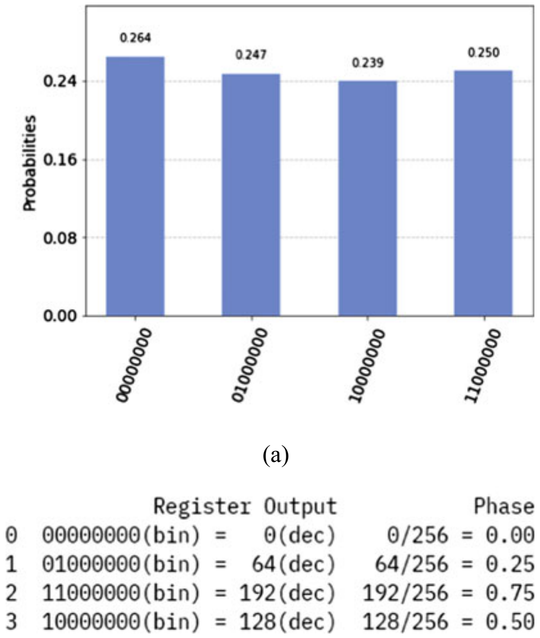


Fig. 12.3 Implementation of order 'r' finding quantum part of Shor's algorithm using IBMQ Qiskit



(a)

```
                 Register Output              Phase
0  00000000(bin) =   0(dec)    0/256 = 0.00
1  01000000(bin) =  64(dec)   64/256 = 0.25
2  11000000(bin) = 192(dec)  192/256 = 0.75
3  10000000(bin) = 128(dec)  128/256 = 0.50
```

(b)

Fig. 12.4 **a** Probability of finding an order for above-described order ‘*r*’ finding quantum part and **b** corresponding measure of phase

measurements of phase is depicted in Fig. 12.4b, the highest phase (0.75) for order $r = 2$. Hence, the order of the given problem is $r = 2$.

12.3 Post-Quantum Algorithm

In most encryption code, symmetric and asymmetric key cryptography is often involved in cryptographic keys. The key distribution mechanism of the cryptographic systems faces challenges to the post-quantum computer era. Quantum key distribution (QKD) or post-quantum cryptographic algorithms bring more attention to the solution of the key distribution mechanism (Bennett and Brassard 1984a, b; Bennet 1992; Bennet et al. 1992; Wooters and Zurek 1982; Wiesner 1983; Bennett et al. 1983; Aaronson 2009; Lutomirski et al. 2009; Farhi et al. 2012; Aaronson and Christiano 2012; Mosca and Stebila 2010; Moulick and Panigrahi 2016; Behera et al. 2017; Chuang and Gottesman 2007; Hillery et al. 1999; https://qiskit.org; https://qiskit.org/textbook/ch-algorithms/shor.html; https://github.com/rubenandrebarreiro/demystifying-the-quantum-key-distribution-scheme-bb84-protocol; Bello et al. 2019; Rarity et al. 2001; Townsend 1994, Townsend et al. 1994; Phoenix and Townsend 1995 Phoenix et al. 1995; Scarani et al. 2009; Gisin et al. 2002; Loepp and Wootters 2006; Gottesman and Chuang 2001). Four-state quantum protocol BB84 (Bennett and Brassard 1984a) and two-state quantum protocol BB92 (Bennet 1992) can let Alice and Bob share the secret key over a quantum channel, always has 50% or 25% probability of miss read by Eve. QKD unconditionally offers secure quantum communication. The most popular QKD protocols are presented as a short state of the art regarding post-quantum cryptography. The motivation for QKD is from the discovery that a quantum computer can factor large numbers in polynomial time. The factorization of large numbers and specific mathematical problems (like the discrete log problem) is considered tough to solve in classical computers.

Charles H. Bennett of IBM and Gilles Brassard of the University of Montreal have proposed the first and most popular QKD protocol known as the BB84 protocol in 1984 (Bennet and Brassard 1984b). Nevertheless, in practical QKD systems, BB84 remains the most well-liked protocol compared to the previously reported protocol (https://qiskit.org/textbook/ch-algorithms/shor.html; https://github.com/rubenandrebarreiro/demystifying-the-quantum-key-distribution-scheme-bb84-protocol; Bello et al. 2019). For this reason, it is employed in a class of cryptographic schemes (Aaronson 2009; Lutomirski et al. 2009; Farhi et al. 2012; Aaronson and Christiano 2012; Mosca and Stebila 2010; Moulick and Panigrahi 2016; Behera et al. 2017; Chuang and Gottesman 2007; https://qiskit.org; https://qiskit.org/textbook/ch-algorithms/shor.html; https://github.com/rubenandrebarreiro/demystifying-the-quantum-key-distribution-scheme-bb84-protocol; Bello et al. 2019; Rarity et al. 2001; Townsend 1994) (comprising public key cryptography) which is based on public key cryptosystems.

The first QKD we demonstrate in the following section is the ‘BB84’ protocol.

12.3.1 BB84 Protocol

BB84 was named after its inventors (Bennett and Brassard), followed by when it was first published. BB84 QKD used the three key principles of quantum computing which are as follows:

1. The no-cloning theorem: Replication of quantum states is not permissible. The generated key never duplicates the quantum states.
2. Measurement led to state collapse: The state will be collapsed when we make measurements of it. Such measures, on the other basis, make entirely random.
3. Processes of measurements are irreversible.

12.3.2 BB84 Protocol Description

We explore the basic idea about the BB84 algorithm, where two bases are considered as Alice and Bob. Alice randomly chooses a basis to create each bit in the string. Alice can choose either $\{|0\rangle, |1\rangle\}$ basis or $\{|+\rangle, |-\rangle\}$, basis to represent ‘n’ qubit key. Now, Alice will send his bases to Bob. Bob will compare it on an arbitrarily chosen basis. If a basis of Alice and Bob is different, then that qubit will be discarded by both of them. As a result, Alice and Bob used different bases of the shifted keys after discarding the qubits. If Eve has tried to eavesdrop on the transmission, then Eve will have a 50/50 chance to choose the right/wrong basis selected by Bob. Hence, half of the information might get changed when Eve copies the information when sent to Bob. Eve is unable to interrupt the communication between Alice and Bob. Now, let us follow the algorithm step by step.

Algorithm BB84:

Step 1: Alice generates bit string ‘*d’* of $(4 + \delta)*n$ random bits 7.

Step 2: Alice chooses another random bit string ‘*b*’ of length $(4 + \delta)*n$. For each bit of the string ‘*d*’, a qubit creates in the Z basis or the X basis according to the bit values of the random string, ‘*b*’.

Step 3: Alice sends the computed bits streams $(4 + \delta)*n$ qubits to Bob (one at a time).

Step 4: Bob receives the $(4 + \delta)*n$ qubits, publicly declares the fact, and measures each bit at random on the Z or X basis.

Step 5: Alice announces the string b that determined the basis she used to encode each bit.

Step 6: Bob discards the measured qubit values obtained if he measured on a basis different from the one that.

Step 7: Alice prepared in. He tells Alice which measurements (but not their results) he discarded. Alice then discards the same set of bits. At least 2n bits are left with high probability; if not, abort the protocol.

Step 8: Alice randomly selects $2n$ bits from the remaining ($\geq 2n$) bits and announces which $2n$ bits she selected (but not their values).

Step 9: Alice randomly selects n of the $2n$ bits to use as check bits and announces this selection of the n bits and their bit values.

Step 10: Bob compares the bit values he measured for, then checks bits selected by Alice, and announces the bits where they disagree. If more than an acceptable number of these check bit values differs, they abort the protocol.

Step 11: Alice now has an n bit string x, and Bob has an n bit string $x + e1$, where $e1$ is the error caused by Eve’s interference and/or channel noise.

Step 12: Alice and Bob perform information settlement, i.e. error correction whereby Bob’s string is corrected to x.

Step 13: Alice and Bob further perform privacy amplification on their n bit strings to obtain k shared key bits.

Table 12.1 BB84 protocol workout example

Alice bits	0	0	1	1	0	1	0	1
Alice basis	{|0⟩ |1⟩}	|±⟩	{|0⟩ |1⟩}	|±⟩	{|0⟩ |1⟩}	|±⟩	|±⟩	{|0⟩ |1⟩}
Bob basis	{|0⟩ |1⟩}	{|0⟩ |1⟩}	|±⟩	|±⟩	{|0⟩ |1⟩}	|±⟩	|±⟩	|±⟩
Match	Yes	No	No	Yes	Yes	Yes	Yes	No
Keep	Yes	No	No	Yes	Yes	Yes	Yes	No

12.3.3 BB84 Protocols Workout Example

In this subsection, we demonstrate the BB84 protocol with the help of a workout example. Let us assume Alice randomly creates eight-bits binary equivalent string ‘00110101’ (practically, it will much larger string). We also assume Alice bases are $|0\rangle|+\rangle|1\rangle|-\rangle|0\rangle|-\rangle|+\rangle|1\rangle$. Bob randomly measures as $|0\rangle|0\rangle|-\rangle|-\rangle|0\rangle|-\rangle|+\rangle|-\rangle$. The following table describes what Alice and Bob will keep as QKD using BB84 protocol (Table 12.1).

As a result, keeping bit positions 1, 4, 5, 6, and 7 and discarded positions 2, 3, 8, we have shift key $s = 01010$. On one occasion, the shift key is generated, and both the parties need to check for errors. Alice will then send this shift key by using a classical communication channel, i.e. via telephone, etc., to Bob. Bob will be able to determine what Alice gets a match with his guess. Finally, Alice and Bob set their QKD for communication $|0\rangle|-\rangle|0\rangle|-\rangle|+\rangle$.

12.3.4 BB84 Protocol Implementation Using IBMQ

Let us now demonstrate the BB84 protocol with IBMQ Qiskit programming. The programme is available in Aaronson and Christiano (2012). We assume Alice randomly chooses 8 bits binary bit string ‘01110101’.

The corresponding basis is as follows:

Alice basis [‘⤢’, ‘⤡’, ‘↕’, ‘↕’, ‘ ↔’, ‘⤡, ‘↔’, ‘↕’].
Here binary 0→ ‘⤢’ basis or ‘↔’ basis.
Binary 1→ ‘↕’ basis or ‘⤡’ basis.
Bob guess basis [‘↔’, ‘↕’, ‘↕’ ‘⤢’, ‘↔’, ‘⤡’, ‘⤢’, ‘⤡’].

Alice bits	0	1	1	1	0	1	0	1
Alice basis	‘⤢’	‘⤡’	‘↕’	‘↕’	‘ ↔ ’	‘⤡’	‘↔’	‘↕’
Bob basis	‘↔’	‘↕’	‘↕’	‘⤢’	‘↔’	‘⤡’	“⤢”	‘⤡’

(continued)

(continued)

Alice bits	0	1	1	1	0	1	0	1
Match	No	No	Yes	No	Yes	Yes	No	No
Binary	0	0	1	0	1	1	0	0
Keep	No	No	Yes	No	Yes	Yes	No	No

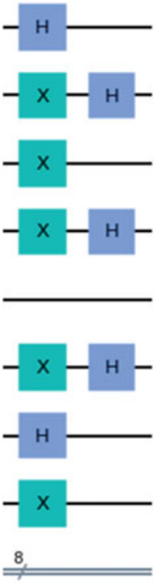
Alice measures 00101100.
Shift key 101.

Recall that polarization state of a photon can be realized to be in one of the following states:

1. Horizontal (spin left/right—↔↔);
2. Vertical (spin up/down—↕↕).

Alice sends this basis using a quantum channel to Bob for QKD establishment. Eve will not measure as the state will be collapsed mentioned in quantum principal 2 mentioned in Sect. 3.1. The implantation quantum circuit is given below (Figs. 12.5, 12.6 and 12.7).

Fig. 12.5 Alice basis



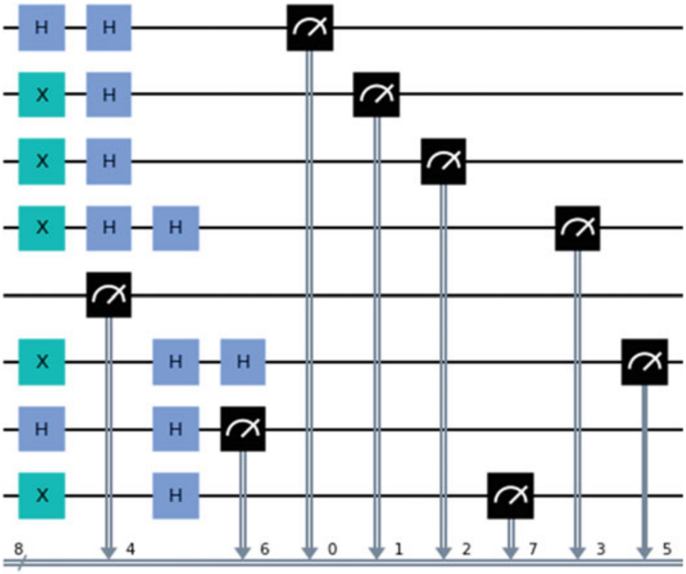
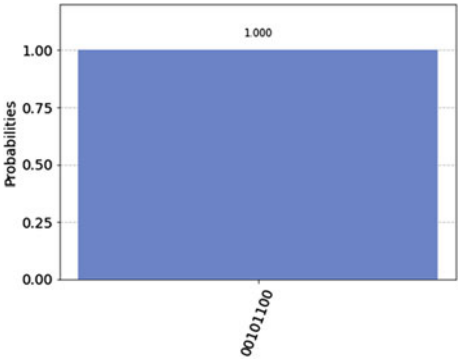


Fig. 12.6 Alice measurement circuit, keep is a classical part of that algorithm

Fig. 12.7 Alice measure binary result to prepare shift key



12.4 Teleportation

In quantum communication, the quantum entangle is being utilized for quantum teleportation. Teleportation is a procedure in which two parties, a quantum state, want to send to Bob by Alice, without being transmitted in the natural sense. Both the parties can set up quantum communication channel as a well classical channel to establish quantum communication by using quantum entanglement. Alice and Bob can perform this task as spooky action using EPR paradox.

Let us start with the basic principle of quantum teleportation. Alice wants to send an unknown state $|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$, only we know that state is normalized, i.e.

$|\alpha|^2 + |\beta|^2 = 1$. Alice and Bob begin to start with entangled pair. The following steps are described teleportation procedure.

Step 1: Both the parties share an entangled pair of particles.
Alice's quantum state '0' denoted by $|0_A\rangle$.
Bob's quantum state '0' denoted by $|0_{\mathrm{B}}\rangle$.
And Alice and Bob create entangled pair.

$$|\psi\rangle = |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_{\mathrm{B}}\rangle + (|1_A 1_{\mathrm{B}}\rangle) \tag{12.6}$$

Step 2: Alice applied CNOT gate with unknown state $|\chi\rangle$

$$\begin{aligned} |\psi\rangle' = |\chi\rangle \otimes |\beta_{00}\rangle &= (\alpha|0\rangle + \beta|1\rangle) \oplus \frac{1}{\sqrt{2}}(|00\rangle + (|11\rangle) \\ &= \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |111\rangle) \end{aligned} \tag{12.7}$$

$$\begin{aligned} |\psi\rangle' &= U_{\mathrm{CNOT}}|\psi\rangle' \\ &= \frac{\alpha}{\sqrt{2}}(U_{\mathrm{CNOT}}|000\rangle + U_{\mathrm{CNOT}}|011\rangle) \\ &\quad + \frac{\beta}{\sqrt{2}}(U_{\mathrm{CNOT}}|100\rangle + U_{\mathrm{CNOT}}|111\rangle) \\ &= \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle) \end{aligned} \tag{12.8}$$

Step 3: Alice applied Hadamard gate

$$\begin{aligned} |\psi\rangle''' = H|\psi\rangle' &= H(\frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle) \\ &= \frac{\alpha}{\sqrt{2}}H|0\rangle((|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}H|1\rangle((|10\rangle + |01\rangle) \\ &= \frac{\alpha}{\sqrt{2}}\frac{(|0\rangle + |1\rangle)}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}(|110\rangle + |101\rangle) \\ &= \frac{\alpha}{2}(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \frac{\beta}{2}(|0\rangle - |1\rangle)(|10\rangle + |01\rangle) \end{aligned} \tag{12.9}$$

Third bit is possessed by Bob.

Step 4: Alice measures her pair.

Equation (12.9) is simplified to

$$|\psi\rangle''' = \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle) \quad (12.10)$$

Alice can measure $|00\rangle\, or |01\rangle\, or |10\rangle\, or |11\rangle$.

Step 5: Alice will send Bob what she measures.

Using classical channel, Alice will disclose her measurement to Bob.

Step 6: Bob will perform the following operation after receiving Alice message.

To get back to the unknown state $|\chi\rangle$.
If Alice measures $|00\rangle$, then.
Bob will do nothing; he possessed an unknown state $|\chi\rangle$.

If Alice measures $|01\rangle$ then.
Bob needs to apply X gate over the state $X\ (\alpha|1\rangle + \beta|0\rangle) = \alpha|0\rangle + \beta|1\rangle = |\chi\rangle$.
Will get back unknown state $|\chi\rangle$.

If Alice measures $|01\rangle$ then.
Bob needs to apply Z gate over the state X $(\alpha|0\rangle - \beta|1\rangle) = \alpha|0\rangle + \beta|1\rangle = |\chi\rangle$.
Will get back unknown state $|\chi$.

If Alice measures $|11$ then.
Bob needs to apply ZX gate over the state ZX $(\alpha|1 - \beta|0) = \alpha|0 + \beta|1 = |\chi$.
Will get back unknown state $|\chi\rangle$.

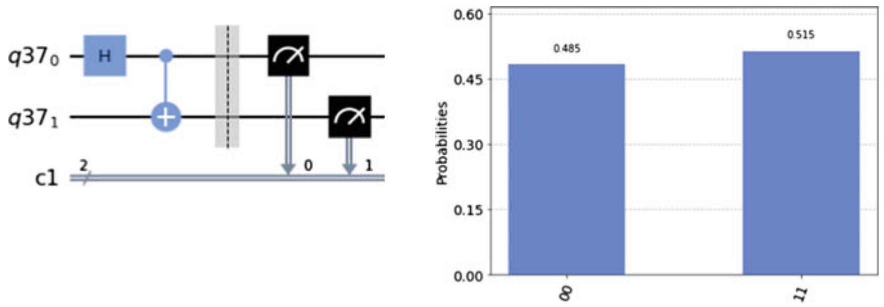
Finally, Alice will be able to send the unknown state to Bob using quantum entanglement.

12.4.1 Teleportation Implementation Using IBMQ

In this subsection, the attempt is made to explore the implementation of quantum teleportation using IBMQ. Let us demonstrate the EPR pair, i.e. entanglement pair of Alice's bit 0 and Bob's bit 0. The following bell circuit and corresponding bell state $|\beta_{00}\rangle$ are known as entangled pair (Fig. 12.8).

The entangled pair is given by Eq. (12.6), 50% probability of being $|00\rangle$ or 50% probability to be $|11\rangle$.

In step 2 and step 3, Alice applies CNOT gate to over unknown pair of $|\psi\rangle' = |\chi\rangle \otimes |\beta_{00}\rangle$, which is represented in Eq. (12.6). The following circuit demonstrates Eq. (12.9) (Fig. 12.9).



(a) (b)

Fig. 12.8 **a** Bell circuit or entanglement circuit **b** bell state or entangled pair

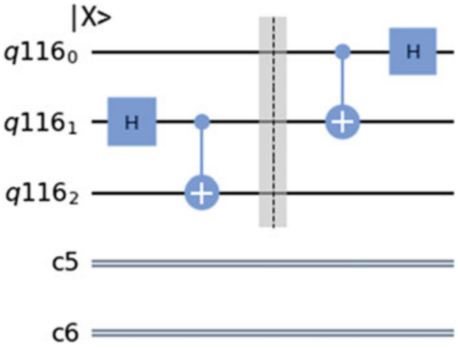


Fig. 12.9 Alice applies CNOT gate to over unknown pair and bell state and Alice apply Hadamard over quantum state $|\psi\rangle''$ as explained in Eq. (12.9)

In step 5:

Alice measures the quantum state $|\psi\rangle''$ as expressed in Eq. (12.10) (Fig. 12.10). Alice will send to Bob what she measures using a classical channel. Alice can measure $|00\rangle$ *or* $|01\rangle$ *or* $|10\rangle$ *or* $|11\rangle$.

In step 6, Bob will apply the following gates to his own possessed qubit; if Alice measures $|00\rangle$ *or* $|01\rangle$ *or* $|10\rangle$ *or* $|11\rangle$, Bob will do the followings.

00 → Do nothing and measures will get unknown state $|\chi\rangle$.

01 → Apply *X* gate and measures will get unknown state $|\chi\rangle$.

10 → Apply *Z* gate and measures will get unknown state $|\chi\rangle$.

11 → Apply *ZX* gate and measures will get unknown state $|\chi\rangle$.

Let us assume Alice measures $|11\rangle$ and Bob will do the following (Fig. 12.11).

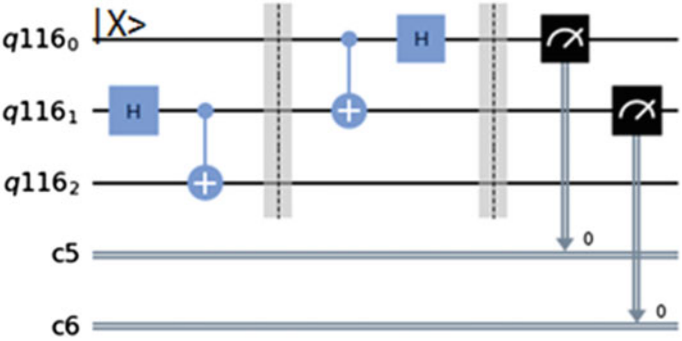


Fig. 12.10 Alice measures the quantum state $|\psi\rangle'''$

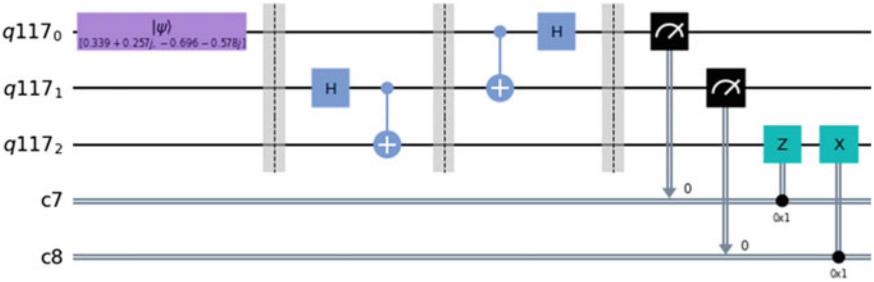


Fig. 12.11 Alice measures $|11\rangle$, Bob applies ZX gate

Before Bob measures the unknown state sent by Alice, Bob uses a disentangler and measures the third bit he possesses (Fig. 12.12).

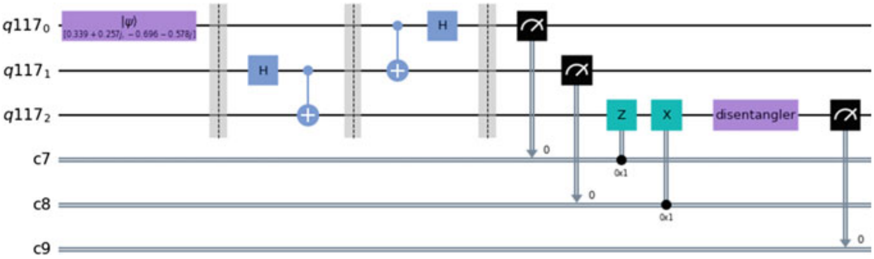


Fig. 12.12 Final measurement of Bob

12.5 Quantum Cheque Algorithm

This section discussed the quantum cheques, an authentic, and secured transaction in quantum banking against any no-signalling adversary. In this secured cryptographic protocol, any valid bank client can generate a cheque that cannot be forged or misused in any case and can be confirmed by the bank or any bank branch.

A considerable annoyance in classical domain is copy protection of classical information. However, the quantum technology domain can regime the copy protection problem, exploiting the 'no-cloning theorem' (Wooters and Zurek 1982). Hence, quantum cheques can play a significant role in banking security. The concept of quantum money was introduced by Wiesner (1983), Bennett and Brassard (1984b), Bennett et al. (1983) in 1969. This cryptographic protocol is based on quantum key distribution, BB84 (Bennett and Brassard 1984b). Wisener's scheme (Wiesner 1983; Bennett and Brassard 1984b) was bounded only to send the messages securely. However, Aaronson's quantum copy protection scheme over BB84 makes quantum security more reliable (Aaronson 2009). A more advanced quantum cryptographic scheme was reported by Lutomirski et al. (2009), Farhi et al. (2012), and Aaronson and Christiano (2012). Side by side, another scheme, quantum coins, was also reported by Mosca and Stebila (2010). Nevertheless, the quantum coin is dependent on the private key protocol, where the scheme is based on blind computation. It means the bank can do the verification process only.

A quantum cheque scheme can provide end-to-end facilities between bank and customer against any no-signalling adversary. A trusted bank can act as a key generator and can store all required documents. A valid customer with 'quantum cheque book' can issue an individual cheque verified by the specific bank. The quantum cheque can provide perfect security bankers end to customer end (Moulick and Panigrahi 2016; Behera et al. 2017).

Again, long-distance quantum communication with quantum analogue cheque technique can be professed as an electronic data interchange for an alternative e-payment gateway. Hardware implementation of the quantum cheque is also reported to verify the algorithm in the IBMQ platform. Three following schemes can accomplish a successful quantum cheque transaction.

Three important properties of quantum cheques are 'Unforgeability', 'Nonrepudiation', and 'Verifiability' (Moulick and Panigrahi 2016; Behera et al. 2017). The 'Unforgeability' indicates that quantum cheques cannot be reused or refabricated. 'Nonrepudiation' means a customer never disclaims the cheque after issuing. Finally, 'Verifiability,' i.e. cheque, can be confirmed by the bank's main branch or any other branches at the same time.

Let us consider three parties, Alice, Bob, and bank, to describe the quantum cheque protocol. Alice and the bank are considered as trusted parties according to protocol. So, firstly Alice has to generate a quantum cheque with the help of the bank. Then, the untrusted party, Bob, goes to bank to withdraw money. After proper verification, bank will transfer the money to Bob. So following three schemes have to follow for a successful transaction. The quantum cheque comprises three algorithms

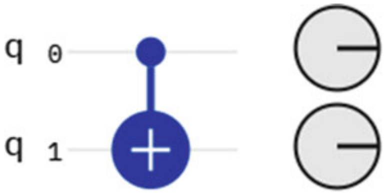


Fig. 12.13 CNOT gate

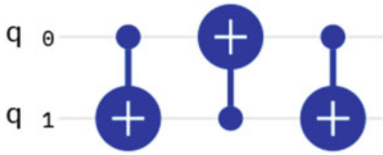


Fig. 12.14 Swap gate

named generation algorithm, digital signature algorithm, and verification algorithm to complete a secured transaction (Moulick and Panigrahi 2016; Behera et al. 2017). Again, the individual scheme can be represented in a quantum gate-level circuit (Behera et al. 2017). Controlled-NOT gate, Hadamard gate, the Pauli gate(X, Y, Z gates), and the phrase gates (S, $S\dagger$, T, and $T\dagger$) are required to implement the quantum cheque (Behera et al. 2017).

CNOT and swap gates are depicted in Figs. 12.13 and 12.14, respectively.

12.5.1 Generation Algorithm

'Generation algorithm' generates a 'quantum cheque book'. Same time a key is generated by the customer, who issues the quantum cheque. Alice and bank prepared a shared key (k) in the initial steps of quantum cheque generation. The valid customer Alice sends a public key (pk) to the bank with a valid customer identification code (id) and collects her private key (sk). After getting a request from valid customer, the bank creates n number of GHZ (Greenberger–Horne–Zeilinger state) states. GHZ state is a simple quantum entangled state which is non-classical properties. For an n qubits system, GHZ states can be represented as Eq. (12.11).

$$|\mathrm{GHZ}\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}} \tag{12.11}$$

For this experiment, 3-bit GHZ states are considered as expressed in Eq. (12.12). Its quantum logic circuit is depicted in Fig. 12.15. Figure 12.16 describes the probability of getting two possible outcomes as defined in Eq. (12.12).

$$|\mathrm{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \tag{12.12}$$

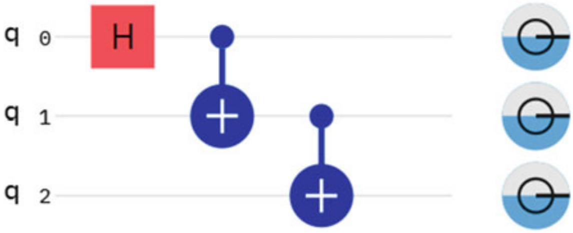


Fig. 12.15 3-qubit GHZ state generator circuit

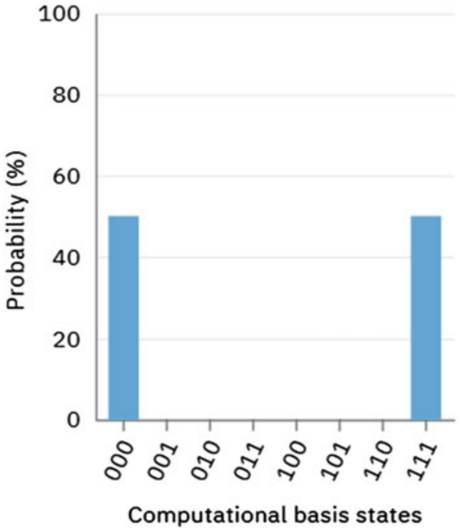


Fig. 12.16 Probability of outcome state of 3-qubit GHZ quantum circuit

Equation 12.11 can also be represented as follows in Eq. (12.13).

$$|\text{Ø}^{(j)}\rangle_{\text{GHZ}} = \frac{1}{\sqrt{2}}\big(|0^{(j)}\rangle_{A1}|0^{(j)}\rangle_{A2}|0^{(j)}\rangle_{\text{B}} + |1^{(j)}\rangle_{A1}|1^{(j)}\rangle_{A2}|1^{(j)}\rangle_{\text{B}}\big) \tag{12.13}$$

where $1 \le j \le n$, with the relevant distinct serial number, i.e. $S \in \{0, 1\}^n$. From every GHZ entangled state, keeping the entangled state $|\text{Ø}\rangle_{\text{B}}$ state securely, the bank returns two qubits, denoted as $|\text{Ø}\rangle_{A1}$ and $|\text{Ø}\rangle_{A2}$ and the serial number to Alice. After generation of quantum cheque, Alice possesses with $\{k, id, pk, sk, S, |\text{Ø}\rangle_{A1}, |\text{Ø}\rangle_{A2}\}$ for the individual entangled state. Same way $\{id, pk, k, S, |\text{Ø}\rangle_{\text{B}}\}$ are stored securely in the bank's end.

12.5.2 Sign Algorithm

Sign algorithm generates a quantum cheque state and quantum cheque (QC). Alice prepares a random number by the procedure $r \leftarrow U\{0,1\}L$ to sign a cheque of amount M. The one-way function, $f{:}\{0,\ 1\} * \ \times\ |0\rangle \rightarrow |\psi\rangle$ creates n-qubit state (Moulick and Panigrahi 2016; Behera et al. 2017; Gottesman and Chuang 2001; Chuang and Gottesman, 2007).

$$|\psi_{\text{alice}}\rangle = f(k||id||r||M)$$

where k and id are the secret keys and the identity of Alice, respectively, the symbol ‘||’ concatenates two-bit strings.

Subsequently, Alice encodes $\left|\psi^{i}_{\text{alice}}\right\rangle$ with the entangled i-th GHZ state, means by either $\left|\varnothing^{i}\right\rangle_{A1}$ or $\left|\varnothing^{i}\right\rangle_{A2}$. After that, a bell measurement is executed on Alice’s first two qubits, as shown in Fig. 12.17 (Behera et al. 2017). Figure 12.18 is the equivalent IBM Qiskit generated circuit of Fig. 12.17. The four particles’ entangled state can be expressed as Eq. (12.14) (Fig. 12.19).

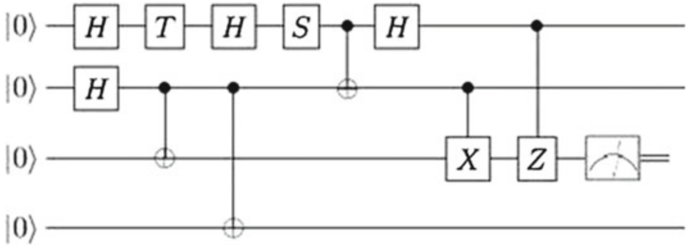


Fig. 12.17 Quantum cheque state generator circuit (Behera et al. 2017)

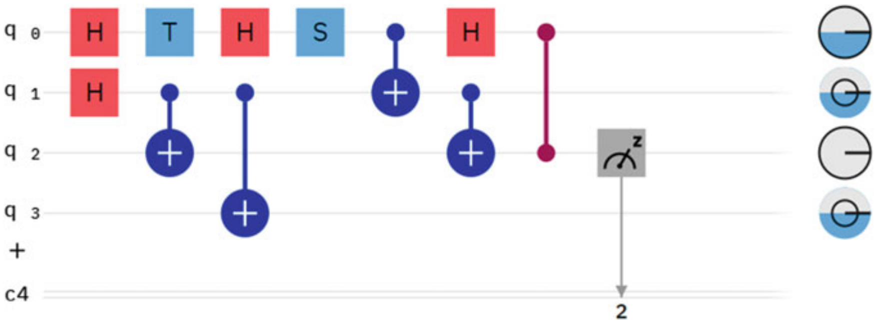


Fig. 12.18 IBM Qiskit generated quantum cheque state generator circuit

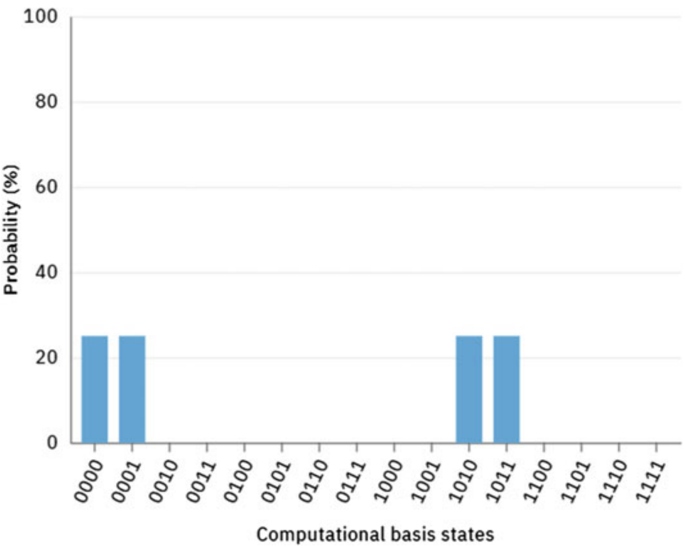


Fig. 12.19 Probability of four possible cheque states generated by Alice

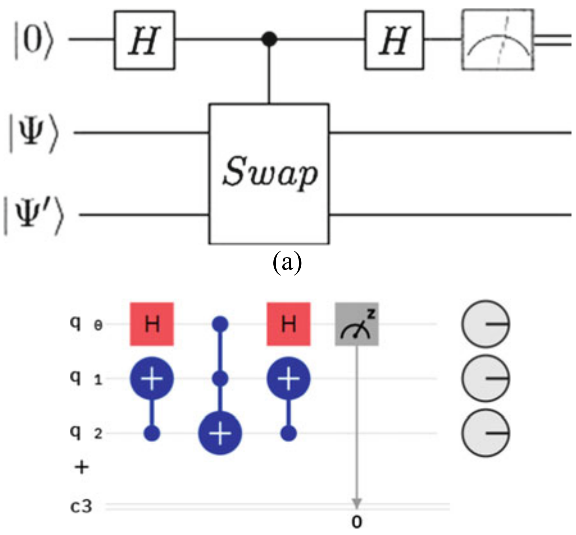
$$\left|\emptyset^i\right\rangle = \left|\psi^i_{\text{alice}}\right\rangle \otimes \left|\emptyset^i\right\rangle_A \tag{12.14}$$

Alice performs proper Pauli gate operations, i.e. I, X, Y, or Z, for error correction (Moulick and Panigrahi 2016; Behera et al. 2017). Figure 12.17 illustrates the encoding procedure of quantum cheque. This encoding process has to continue n times. Finally, Alice signed on the quantum cheque using the signature algorithm (Gottesman and Chuang 2001; Chuang and Gottesman 2007) for the unique serial number S as $\sigma \leftarrow \text{Sign}_{\text{sk}}\,(S)$. Now quantum cheque is ready to use in the following form QC $= (id,\ S,\ r,\ \sigma,\ M,\ \left\{\left|\emptyset^i\right\rangle_A\right\}_{i=1:n}$. Now Bob can submit this cheque to the specific bank or branches for encashing.

(a) Verification Algorithm

The verification algorithm verifies the validity of a quantum cheque. Bob submits the quantum cheque (QC) in any acting branch. The branch office communicates with the bank's main branch to verify the (id, S) pair. The verification is processed by using $V_{pk}(\sigma, S)$. If the verification process finds the valid pair (id, S) and σ, then the next cycle will commence. Otherwise, the transaction will be terminated.

Then the main branch of the bank measures GHZ state $\left|\emptyset\right\rangle_{\text{B}}$ in Hadamard basis to obtain output, i.e. $|+\rangle$ or $|-\rangle$. The result forwards to the acting branch, and the acting branch applied proper Pauli gates on $\left|\emptyset^{\text{i}}\right\rangle_A$ to recover the unknown state $\left|\psi^i_{\text{alice}}\right\rangle$. This process continues n times to recover $\left|\psi^i_{\text{alice}}\right\rangle_{i=1:n}$ for each value of i. Now using a one-way function, acting branch computes $\left|(\psi^i_{\text{alice}})'\right\rangle$ and then performs a swap test on each of $\left|\psi^i_{\text{alice}}\right\rangle$ and $\left|(\psi^i_{\text{alice}})'\right\rangle$. The quantum circuit of the swap test is depicted in Fig. 12.20a and b.



(a)

(b)

Fig. 12.20 **a** Block diagram of swap test circuit (Behera et al. 2017), **b** equivalent quantum circuit of the swap test circuit

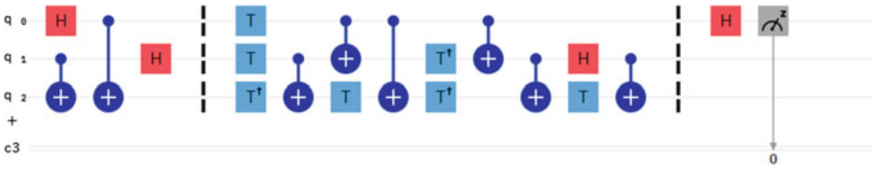


Fig. 12.21 IBM quantum cheque verification circuit

Finally, the bank recognizes the cheque if it passes the swap test, i.e. $\langle \psi^i_{\text{alice}} | (\psi^i_{\text{alice}})'_{i=1:n} \rangle \geq \lambda$, where λ means threshold value determined by bank (Moulick and Panigrahi 2016; Behera et al. 2017). If it does not pass the swap test, then bank rejects the request and aborts the transactions. The quantum cheque verification circuit is depicted in Fig. 12.21.

12.6 Conclusion

In this chapter, we present the main challenges in classical cryptography in the post-quantum era. Current encryption code will face the question of how it can be secured in the near future. Shor's algorithm shows the power of quantum computers, which can decode our present encryption algorithms. Quantum computer developments lead us to think about post-quantum encryption algorithms, i.e. key distribution techniques in a post-quantum era. BB84 and BB92 described the quantum key distribution techniques to protect our data communication and transactions post-quantum age.

The idea of quantum currency bonds, i.e. secure quantum cheques, is presented utilizing different quantum states. A GHZ state and a classical bit string are required as secret keys to complete a transaction (Moulick and Panigrahi 2016; Behera et al. 2017). The quantum cheque scheme (Moulick and Panigrahi 2016; Behera et al. 2017) is unconditionally secure based on quantum theorem, i.e. Holevo's theorem, the signalling theorem, and the no-cloning theorem. Conventionally, the digital signatures model is primarily a two-party protocol, whereas the quantum cheque has a three-party protocol. This three-party protocol enhances transparency and security in comparison with classical currency methods. Hence, these quantum cheque methods will play a crucial role in the much-anticipated quantum Internet as payment gateways.

References

Aaronson S (2009) Quantum copy-protection and quantum money. In: Proceedings of 24th annual IEEE conference on computational complexity (CCC). IEEE, pp 229–242

Aaronson S, Christiano P (2012) Quantum money from hidden subspaces. In: Proceedings of the 44th annual ACM symposium on theory of computing, ACM, pp 41–60

Behera BK, Banerjee A, Panigrahi PK (2017) Experimental realization of quantum cheque using a five-qubit quantum computer. Quantum Inf Process 16(12):312

Bello L, Challenger J, Cross A, Faro I, Gambetta J, Gomez J, Javadi-Abhari A, Martin P, Moreda D, Perez J, Winston E, WoodC, QISKit, originally authored by, https://github.com/QISKit/qiskit-sdk-py and https://quantum-computing.ibm.com/

Bennet CH (1992) Quantum cryptography using any two non-orthogonal states. Phys Rev Lett 68:3121–3124

Bennet CH, Bessette F, Brassard G, Salvail L, Smolin J (1992) Experimental quantum cryptography. J Cryptol 5:3–28

Bennett CH, Brassard G (1984a) Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers, systems and signal processing, Bangalore, India, pp 175–179, Dec 1984a

Bennett CH, Brassard G (1984b) Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers, systems, and signal processing. Bangalore, India, pp 175–179

Bennett CH, Brassard G, Breidbart S, Wiesner S (1983) Quantum cryptography, or unforgeable subway tokens. In: Chaum D, Rivest RL, Sherman AT (eds) Advances in cryptology, Springer, Berlin, pp 267–275

Chuang I, Gottesman D (2007) Quantum digital signatures. US Patent 7246240, 17 July 2007

Farhi E, Gosset D, Hassidim A, Lutomirski A, Shor P (2012) Quantum money from knots. In: Proceedings of the 3rd innovations in theoretical computer science conference. ACM, pp 276–289

Gisin N, Ribrody G, Tittel W, Zbinden H (2002) Quantum cryptography. Rev Mod Phys 74:145–195

Gottesman D, Chuang I (2001) Quantum digital signatures. arXiv:quant-ph/0105032.

Hillery M, Bužek V, Berthiaume A (1999) Quantum secret sharing. Phys Rev A 59(3):1829

https://github.com/rubenandrebarreiro/demystifying-the-quantum-key-distribution-scheme-bb84-protocol

https://qiskit.org

https://qiskit.org/textbook/ch-algorithms/shor.html

Loepp S, Wootters WK (2006) Protecting information: from classical error correction to quantum cryptography. Cambridge University Press, New York

Lutomirski A, Aaronson S, Farhi E, Gosset D, Hassidim A, Kelner J, Shor P (2009) Breaking and making quantum money: toward a new quantum cryptographic protocol. arXiv: 0912.3825

McMahon D (2007) Quantum computing explained. Wiley

Mosca M, Stebila D (2010) Quantum coins. Error Correct Codes Finite Geom Cryptogr 523:35–47

Moulick SR, Panigrahi PK (2016) Quantum cheques. Quantum Inf Process 15:2475–2486

Phoenix SJD, Barnett SM, Townsend PD, Blow KJ (1995) Multi-user quantum cryptography on optical networks. J Mod Opt 42(6):1155–1163

Phoenix SJD, Townsend PD (1995) Quantum cryptography: protecting our future networks with quantum mechanics. In: Cryptography and coding: 5th IMA conference (Dec. 1995), pp 112–131

Rarity JG, Gorman PM, Tapster PR (2001) Secure key exchange over 1.9 km free-space range using quantum cryptography. Electron Lett 37(8):512–514

Rosen KH, Krithivasan K (2012) Discrete mathematics and its applications: with combinatorics and graph theory. Tata McGraw-Hill Education

Saxena S, Sanyal G, Srivastava S et al (2017) Preventing from cross-VM side-channel attack using new replacement method. Wireless Pers Commun 97:4827–4854. https://doi.org/10.1007/s11277-017-4753-7

Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dusek M, Lutkenhaus N, Peev M (2009) The security of practical quantum key distribution. Rev Mod Phys 81:1301–1350

Townsend PD (1994) Secure key distribution system based on quantum cryptography. Electron Lett 30(10):809–811

Townsend PD, Phoenix SJD, Blow KJ, Barnett SM (1994) Design of quantum cryptography systems for passive optical network. Electron Lett 30(22):1875–1877

Wiesner S (1983) Conjugate coding. ACM Sigact News 15(1):78–88

Wooters W, Zurek W (1982) Quantum no-cloning theorem. Nature 299:802