The IoT in Security Architecture, Challenges, and Solutions

Anita Punia, Manish Tiwari, and Sourabh Singh Verma

Abstract The Internet of Things (IoT) is a forerunner to the smart world, as it uses ubiquitous computers and networking to simplify and supply other services, such as easy monitoring of many phenomena in our environment. Environmental and everyday goods referred to as things, objects, or machines, are improving with computing and communication technologies in the Internet of Things. An IoT architecture may provide a variety of solutions for various industries, but its primary goal is to establish a functioning, scalable, flexible, maintainable, and cost-effective IoT ecosystem. This paper analyses the challenges of security and their solutions and presents well-defined security architecture as confidentiality of the privacy and security of the user, which could result in its wider mass acceptance.

Keywords Internet of things · Privacy · Confidentiality · Security · Challenges

1 Introduction

The Internet of Things is a rather straight forward concept: it entails linking all physical places and things on the planet to the internet. IoT is one of the impending ideas of mechanical advancement in the field of organizations, which is help not just in the modern turn of events yet additionally in the everyday existence of an individual. The internet of Things (IoT), is an arranged interconnection of ordinary items of sensors fully intent on interfacing with everything [1]. The methods of protection employed to secure internet-connected or network-based devices are referred to as

M. Tiwari · S. S. Verma
Department of Electronics and communication Engineering, Manipal University Jaipur, Jaipur, India
e-mail: manish.tiwari@jaipur.manipal.edu

S. S. Verma
e-mail: ssverma80@gmail.com

A. Punia (✉)
Department of Computer and communication Engineering, Manipal University Jaipur, Jaipur, India
e-mail: annubhariya@gmail.com

M. Tiwari et al. (eds.), *Optical and Wireless Technologies*, Lecture Notes in Electrical Engineering 892, https://doi.org/10.1007/978-981-19-1645-8_42

Table 1 A comparison of previous papers

Reference	Architecture	Technology	Security	Applications	Protocols for information
[1]	√	√	√	×	×
[5]	√	√	√	×	×
[7]	√	√	√	×	×
[9]	√	√	√	√	×
[10]	√	×	√	√	×
[11]	√	√	√	√	×
[12]	√	√	√	√	×
[13]	√	×	√	×	√
[14]	√	×	√	√	×
[15]	√	×	√	√	×
[16]	√	√	√	√	×
[17]		√	√	√	√
[18]	√	√	√	√	√

IoT security. The internet of things (IoT) refers to a situation in which all objects are connected to the internet via information sensing devices for intelligent identification and management [2]. The essential objective of this article is to give a comprehension of IoT security concerns. A human with a heart monitor implant, a farm animal with a biochip transponder, or some other man-made object with a specific IP address and the ability to link to the network for data transmission can all considered things in the internet of things [3]. This paper discusses a high-level overview of the Internet of Things, including its architecture, threats, and security issues. Concerns about security issues theoretically, these problems are investigated using criteria such as authenticity, integrity, availability, and confidentiality. To show the on-going study, we use to filter the number of publications from 2013 to 2018. The various publications in emerging IoT applications are shown in Fig. 1. Many engineering opportunities have arisen because of the rapid growth of IoT technology. The rapid development of IoT technology has generated numerous engineering and scientific opportunities as well as challenges. It calls for increased research efforts from a variety of industries, including academia, business, and government. The combined efforts of these sectors should inevitably result in the creation of new protocols, architectures, and services that are desperately needed to meet the IoT's challenges. The paper is organized as; the architecture of IoT has been presented in Sect. 2. The security risks are discussed in Sect. 3. Section 4 focuses on the security issues, parameters, and solutions that IoT faces. Finally, Sect. 5 summarizes the paper with a conclusion (Table 1).

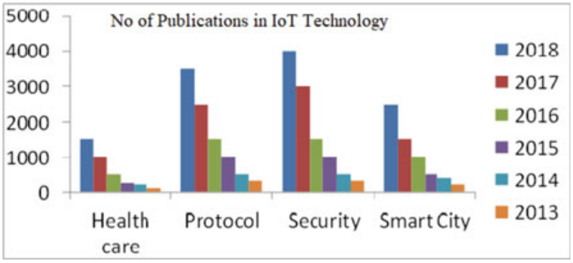

Fig. 1 The number of publications in the areas of IoT protocols, security, and emerging applications is increasing

2 IoT Architecture

The principal concepts of the Internet of Things are characterized by the four-layer architecture. The phrase "internet of things" is made up of two words: "interconnected networks" and "things," which demonstrate certain artifacts. However, at the point when these two terms are combined, they form a “global network of networks. Interconnected objects, each with its unique address, are based on a protocol for regular communication [4]. The layered architecture of IoT is described in this paper, which gives an idea of the fundamental architecture of IoT. The perception layer, Network layer, procession layer and Application layer are the layers that make up IoT [5, 6]. As seen in Fig. 1, all four layers have a large amount of data and different enabling technologies and functionality.

(i) **The perception layer:** The principal layer of IoT engineering is this. An assortment of sensors and actuators are utilized in the insight layer to gather helpful data like temperature, dampness content, interloper location, vibrations, etc.
(ii) **The network layer:** The layer ties the vision and middleware layers, as the name infers. It utilizes organizing advances like 3G, 4G, UTMS, Wi-Fi, and others to get information from the discernment layer and move it to the middleware layer.
(iii) **The procession layer:** The Middleware Layer contains progressed highlights like stockpiling, calculation, handling, and activity taking. It saves all information and sends it to the suitable PC dependent on the gadget’s location and name.
(iv) **The application layer:** Given data assembled from the middleware layer, the application layer handles all application measures. Sending messages, setting off cautions, security frameworks, turning on or off gadgets, brilliant watches, shrewd horticulture, and different assignments are all important for this application.

The list of several IoT technologies used to complete our analysis of the IoT architecture models. Similar layers of architecture (Table 2).

Table 2 IoT technologies

Communication technologies	
Short-range	RFID, Zig Bee, ANT, Z-Wave, NFC, Bluetooth, ANT
Medium range	QR Code, WiMAX, DASH7, Ethernet, EnOcean
Long range	3G/4G, GPRS, Satellite GPS, LTE, G Lora WAN GSM.
Prototype hardware	
Arduino Yun, Raspberry Pi, Arduino Uno, Hackberry, PCDuino, Cubie Board, The Rascal, Pinoccio , Beagle Bone Black, Pinoccio, Pinoccio	
Operating system	
Nano-RK, Tiny OS, Contiki, Mantis, Free RTOS, SNAP OS, Abacus OS	
Protocol	
6LoWPAN, REST, MQTT, LoRa, DTLS, Lora WAN, XMPP-IoT, SSI	

3 IoT Challenges

3.1 Security Threats and Challenges in the Internet of Things

There are three types of IoT risks:

1. Risks that is characteristic of any device on the internet.
2. Risks associated with IoT device.
3. Protection to ensure that no damage is caused, for example, by misuse of actuators.

Standard security rehearses, for instance, getting open ports on contraptions to have a spot with the essential arrangement (for example, a fridge related to the Internet to send alerts about the thing stock and temperature may use an unsteady SMTP labourer and can be sabotaged by a botnet). We will shortly audit some principle challenges.

Scalability: Scalable security solutions are needed to handle a great number of IoT nodes.

Connectivity: Another difficulty in IoT communications is to connect various ML / Devices with different capabilities in a safe manner.

End-to-End Security: OSCORE involves the use of a key exchange protocol to create a security context. However, this protocol should take into account the needs of restricted scenarios (e.g., LPWAN), as well as end-device computation and storage limitations [13].

Authentication and Trust: This forestalls a certainty connection between IoT elements from being formed, which is essential for IoT applications requiring specially appointed contact, such as the Smart City scene, between IoT components.

Identity Protection: Management of identity is a challenge because bad security practices are often enforced. For instance, a common mistake is the use of clear text/Base64 encoded device/machine-to-machine (M2M) IDs/passwords.

Attack-Resistant Security Solutions: IoT system diversity results in a need for security solutions that are attack-resistant and lightweight. They are defenceless against asset enervation assaults because IoT gadgets have restricted processing assets.

3.2 Threats and Attacks on IoT Security

To underline security risks in IoT, its shortened form has been presented as Interconnection of Dangers (IoT). Undoubtedly, IoT gadgets are especially powerless against actual attacks, programming attacks, side-channel attacks, etc. as introduced in Table 3.

Present IoT platforms are made up of a range of technology solutions from different vendors. Any of these frameworks are a diverse blend of segments repurposed from existing answers for use in uniquely fabricated stages in the expectation that the parts can cooperate securely.

Table 3 Security threats to IoT devices

Threats	Procedure for an attack	Security requirement	Examples
Physical attack	Play with the equipment and different pieces of the framework	Resistance to tampering	Micro-probing of layout reconstruction
Environment attacks	By recovering the encryption information, the attacker will discover the system encryption key.	Encryption system that is secure	Attacks on pacing, side channels, and analysis fault attack
Cryptanalysis attacks	To decrypt the data, look for cypher text.	Encryption system that is secure	Plaintext attack (known plaintext) and plaintext attack (chosen plaintext)
Software attacks	Exploit device vulnerabilities and inject malicious code into the system's own communication interface	Update antivirus software	Viruses , worms or Trojan horse are all examples of malicious software

Table 4 Taxonomy of attacks based on IoT process phases

Phase	Attack/Threat	Description
Data Collection: There are several different types of data gathering that can be used. A static (body sensors) might be utilized as the unit (sensors and chips)	Breach or Data Leakage information Authentication information Sovereignty, and information Loss, are all issues that need to be addressed	Internal or external data leakage may occur, and it can be deliberate or unintentional. Is it software or hardware
Storage: Data are often saved if the pc has its native memory. The information from homeless devices are often protected to the cloud	Accessibility, Access Control, Genuineness, Forswearing of Administration, and Detainment are for the most part instances of assaults on accessibility, access	The over-burden condition initiated by an enormous number of conveyed aggressors is known as distributed denial of service
Intelligent processing	Authentication attack	In real-time, an IoT solution offers information processing
Transmission of data	Session hijacking, flooding of the channel security, steering conventions	Interruptions, blocking, data manipulation, forgery
End-to-end term	Man or computer that is the question. Maker or thief	On-time delivery of stored data with no mistakes or alterations

3.2.1 Attack Classification for IoT Interaction Stage

An IoT approach can be thought of as a five-phase series, starting with data collecting and ending with data transmission to end users. Table 4 indicates the spectrum of assaults categorized for the five IoT phases: interpretation of data, storage, smart processing, transmission of data and end-to-end delivery [7].

3.2.2 Categorization of Attacks Based on IoT Architecture

There are different IoT models of architecture, as mentioned in Sect. 2. In general, four layers are believed to have the IoT architecture, presented in Fig. 2. At the awareness, network, and service levels, we will take a quick look at the biggest security threats. Table 5 summarizes the most significant security issues in the IoT provided as four-layer architecture (Fig. 2).

3.2.2.1 Threats to Security at the Sensing and Perception Layer

It should be customized and introduced into the actual gadgets to authorize IoT security. This implies IoT gadgets should have the option to demonstrate their character, hold their realness, sign, and encode their information to keep up with believability, and to ensure protection by confining information that is saved locally. The situation security model should be adequately unbending to forestall unapproved use while as yet being sufficiently adaptable to work with secure specially appointed interchanges with people and different gadgets on an impermanent premise [8].

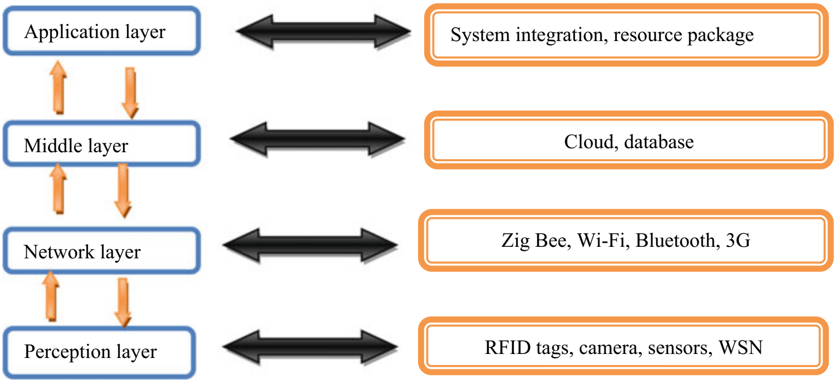
Application layer
System integration, resource package
Middle layer
Cloud, database
Network layer
Zig Bee, Wi-Fi, Bluetooth, 3G
Perception layer
RFID tags, camera, sensors, WSN

Fig. 2 Architecture of IoT

Table 5 Top Ten Vulnerabilities in IoT

Corners of security	Interface & application layer	Service support layer	Middleware/network layer	Unit/device layer
Online interface that is not stable	√	√	√	
Inadequate authentication and authorization	√	√	√	√
Network facilities that aren't stable		√	√	
Transport encryption isn't available		√	√	
Privacy nooks		√	√	√
Cloud interface that is unreliable	√			
The mobile app is insecure	√		√	√
Configuration of security is insecure	√	√	√	
Software/firmware that isn't stable	√		√	
Inadequate physical defence			√	√

Harm to Physicality: Some attackers can lack technological expertise and the destruction of devices limits their attacks. As device enclosures are often not tamper-proof, it is possible to open the devices, access their hardware through probes, and pin headers.

Capturing Node: Instead of destroying them, the information stored on the devices will be stolen by an active attacker.

Attack of the Sinkhole: They become defenceless against sinkhole assault if sensors are left unattended for significant stretches in the organization.

Attack Selective Routing: Malicious nodes can pick, drop packets, thus selectively filtering thus, some packets are selectively filtered, and the rest enabled.

Witch Strike: On the off chance that a noxious IoT hub exploits a genuine hub's disappointment, If rouge IoT hub exploits a genuine hub's disappointment, this attack occurs.

3.2.2.2 Security Threats

Layers of Network and Service Support
The IoT management framework is defined by the administration support layer (Fig. 2) and is liable for installing gadgets and clients, executing approaches and guidelines, and coordinating computerization across gadgets. At this stage, role-based access control to monitor the identity of users and devices and the actions they are allowed to take is important.

Attack by Man-in-the-Middle (MITM): Assault by Man-in-the-Middle (MITM). The Man-in-the-middle assault is a representation of the IoT's latent capacity snooping. Since device authentication requires device identity sharing, identity theft involves identity theft. All dangers of assaults on IoT frameworks should go through the mist layer in the center, which can detect and mitigate suspicious activities before they reach the device [12].

Attack Replay: This data might be ridiculed, adjusted, or replayed during the exchanging of character-related information or various certificates inside the IoT.

Denial of Service Attack: An interloper could dodge the firewall and dispatch a refusal of administration (DoS) assault, delivering the route administration difficult to reach, or convey a bogus message, driving the driver as plate [11]. In addition, most IoT developers have an embedded programming history, which makes them unaware of IoT programming and risks. Attackers could gain access to the keen home arrange and send mass messages to shrewd gadgets, like Solicitation To Send (RTS)/ Clear To Send (CTS) [15].

4 IoT Security parameters

Protection must be handled from the initial design to the services operating in the IoT lifecycle. For example, during device manufacturing, the execution of safety highlights should start.

Code marking and code confusion are a few stages that makers should take to guarantee that their device is not compromised or that a malicious user does not insert unauthorized code. Data confidentiality, safety, and trust are the key security criteria in IoT scenarios, as shown in Fig. 3. Protection is required for IoT systems as a result of IoT security issues. As a result, based on conventional security criteria, it is vital to fabricate a protected web arrangement of things, which are as per the following [19]:

4.1 IoT Solutions

The engineering of the IoT is a major method of planning the various components of the IoT so it can give network benefits and fulfil future requirements. Sensors, actuators, entryways, conventions, cloud administrations, organizations, and application workers are all essential for the IoT design, which are coordinated in different geographies to speak with each other [16]. The term "Internet of Things" refers to a large and diverse ecosystem that encompasses a wide range of connectivity kinds and application cases. As a result, discussing the IoT ecosystem as a whole is ineffective, and understanding IoT requires breaking it down into layers [20]. The fourth industrial revolution will be built on sensors and actuators. They have already altered how people view their surroundings. From urban planning to social consciousness, sensor-enabled smart cities are paving the way for a more sustainable future [21].

The following are the primary IoT phases (layers) that include the IoT architecture solution (Fig. 4).

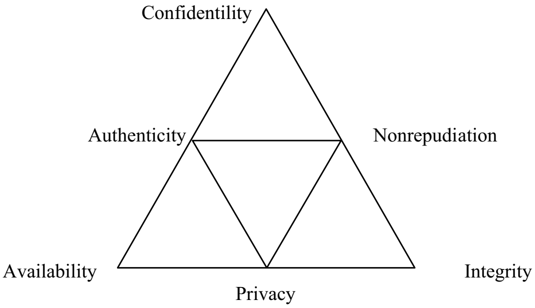

Fig. 3 Security requirements in the internet of things

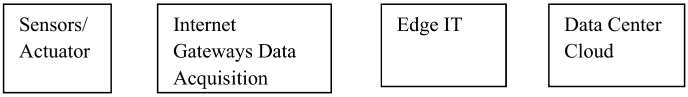

Fig. 4 Solutions of IoT

i. **Sensors/Actuators**
The instruments that can emit, receive and process data over the network are sensors or actuators. This includes GPS, electrochemistry, gyros copy, RFID, etc. Most of the sensors need connectivity through gateways to the sensors. A Local Area Network (LAN) or Personal Area Network may be used for connecting sensors or actuators. The sensor is in charge of detecting and collecting the analogy signals that represent environmental data. Analog signals are converted to digital data by the analog-to-digital converter, which then passes the data to the processing unit [22].

ii. **Gateways and Data Acquisition**
Because these sensors and actuators generate vast volumes of data, high-speed gateways and networks need to transfer data. The type of this network may be Local Area Network (LAN, such as Ethernet, Wi-Fi and so forth), Wide Area Network (WAN like 5G, GSM and so on). This framework was created to allow for the capture of multimodal data from a variety of sources and data providers, as well as to address current connectivity and communication challenges [23].

iii. **Edge IT**
Edge is the equipment and programming entryway in IoT Engineering that investigates and pre-measures information before moving it to the cloud. Edge figuring is a moderately late idea in the registering scene. It brings distributed computing administrations and utilities nearer to the end client, and quick handling and application reaction times portray it [24].

iv. **Data Center/Cloud**
Management Systems that process information through analytics, system management, and security controls are part of the Data Center or Cloud. A server farm is an area where establishments' PCs and related hardware, like peripherals, are kept up. Universities, businesses, national laboratories, hospitals, research institutes, government agencies, and other institutions could be among them [25].

5 Conclusion

The design of IoT security allows for a free, widespread infrastructure with interoperability. We conclude this paper by stating that, following the identification of the key IoT-enabling technologies, challenges, parameters, and solutions, The creation of the network architecture and framework to efficiently handle future IoT applications is the next step. Furthermore, IoT systems are implementing a variety of important technological advancements in a variety of industries. To safeguard their connected devices from malicious assaults, several suppliers and enterprises implement a variety of restrictions. More privacy and security issues have been raised as more of these gadgets are connected to our private networks and the Internet. When it comes to protecting IoT-based systems and devices, security should be a primary focus. To secure their systems from potential threats, businesses should consider implementing numerous levels of protection. IoT data may be processed using modern analytical tools like Artificial Intelligence and Machine Learning to improve security. Blockchain is a promising solution for data security in IoT-enabled ecosystems, as it eliminates the need for central permission in the IoT network.

Reference

1. Conner M (2010). Sensors empower the “Internet of Things”, pp 32–38. ISSN 0012-7515
2. Shao X (2012) Study on security issue of internet of things based on RFID. In: Fourth international conference on computational and information sciences
3. http://whatis.techtarget.com/definition/Internet-of-Things
4. INFSO D.4 (2008) Networked Enterprise & RFID INFSO G.2 Micro & Nano systems, in: co-operation with the working group RFID of the ETP EPOSS. Internet of Things in 2020, roadmap for the future, version 1.1
5. Xu X (2013) Study on security problems and key technologies of the internet of things. In: International conference on computational and information sciences
6. Yan L, Zhang Y, Yang LT (2008) The Internet of Things: from RFID to the next-generation pervasive networked systems. Auer Bach Publications
7. https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2018KS_Gloukhov
8. https://it.b-ok2.org/book/3307183/d60844
9. Hany AF, Gary WB (2019) IoT security, privacy, safety and ethics, digital twin technologies and smart cities. Springer Cham, pp 123–149
10. Anca JD, Pasika R, Xu L (2019) Introduction to IoT security. John Wiley Sons Ltd., Hoboken, pp 1–37
11. Shapla K, Ismail AB, Mohd IIY, Mohamed JH, Bin SM, Aznul G (2020) A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access 8:219709–219743
12. Vikas H, Vinay C, Vikas S, Divyansh J, Pranav G, Biplab S (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7:82721–82743
13. Pérez Salvador L, José R-H, Shahid R, Antonio S (2020) Application layer key establishment for end-to-end security in IoT. IEEE Internet Things J 7(3):2117–2128
14. Hui S, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. In: International conference on computer science and electronics engineering. IEEE, pp 648–651
15. Gil HS, Razzaq AM, Qureshi AM, Ullah S (2017) Security issues in the Internet of Things (IoT): a comprehensive study. (IJACSA) Int J Adv Comput Sci Appl 8(6)
16. Iqbal W, Abbas H, Daneshmand M, Rauf B, Bangash YA (2020) An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet Things J 7(10):10250–10276
17. Meneghello Francesca, Calore Matteo, Zucchetto Daniel, Polese Michele, Zanella Andrea (2019) IoT: Internet of Threats? a survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J 6(5):8182–8201
18. Pallavi S, Smruti RS (2017) Internet of Things: architectures, protocols, and applications. J Electr Comput Eng, 1–25
19. Bhabad MA, Bagade ST (2015) Internet of Things: architecture, security issues and counter-measures. Int J Comput Appl (0975– 887) 125(14), 1–4
20. El Ahmed H (2018) Internet of Things (IoT) system architecture and technologies. Research, pp 1–3. https://doi.org/10.13140/RG.2.2.17046.19521
21. Mohammad H, Mounir A (2018) Sensors and actuators in smart cities. J Sensor Actu Netw MDPI 7:1–4
22. Wen ST (2010) Multi-sensors data fusion system for wireless sensors networks of factory monitoring via BPN technology. Expert Syst Appl 7:2124–2131

23. Perakis K, Miltiadou D, Nigro A, Torelli F, Mantas L, Magdalinou A, Mavrogiorgou A, Kyriazis D (2019) Data sources and gateways: design and open specification. Acta Informatica Medica 27(5):341. https://doi.org/10.5455/aim.2019.27.341-347
24. Wazir KZ, Ejaz A, Saqib H, Ibrar Y, Arif A (2019) Edge computing: a survey. Future Gener Comput Syst 97:1–40
25. Michael PJ, Aparna VS, Stefan RA (2015) The greening of data centers with cloud technology. Int J Cloud Appl Comput 5(4):1–23