Chapter 12
Security and Privacy Issues in Fog Computing for Healthcare 4.0

Shivani Desai, Tarjni Vyas, and Vishakha Jambekar

12.1 Introduction

Fog computing bridges the gap between sensors and analytics in healthcare. As it is a distributed system, application-specific logic does not only reside in the cloud or devices but also onto different components of network. For example, gateways, routers access points, and the devices which are placed over the human body. The healthcare 4.0 is more towards using the standard technologies of IT field like cloud computing, machine learning, big data, Fog computing. Such a system maintains medical connectivity globally and gets access to it whenever required. Fog computing is the interworking of different objects. Network connectivity allows this object to communicate and exchange related information which includes sensors, smartphones, smart meters, radio frequency identification, and other such IoT devices that are useful in health applications. This interconnectivity expands the automation of human's daily life. Its decentralized infrastructure utilizes various IoT devices which collaboratively perform different tasks like communication, computation, storage, control, and management. This arises the new challenges in security and privacy issues. The privacy of patient's data is at most a high priority. Also, the transfer of such information, the privacy of data, and accessing information are major issues. Trust issues of Fog nodes arise as Fog computing network is deployed by various nodes of that network which will not be completely trusted as devices are susceptible to different attacks. The Fog devices have constraint storage, computing, and resources and are easy to be hacked. Therefore, different tools and

S. Desai (✉) · T. Vyas · V. Jambekar
Institute of Technology, Computer Science and Engineering Department, Nirma University, Ahmedabad, India
e-mail: shivani.desai@nirmauni.ac.in; tarjni.vyas@nirmauni.ac.in; 19mcei02@nirmauni.ac.in
http://www.nirmauni.ac.in

S. Tanwar (ed.), *Fog Computing for Healthcare 4.0 Environments*,
Signals and Communication Technology,
https://doi.org/10.1007/978-3-030-46197-3_12

protocols are used to secure the communication channel of the device as well as data. Legal and privacy-related issues, lack of transparency, cybersecurity issues are also the most important challenges need to be solved [1].

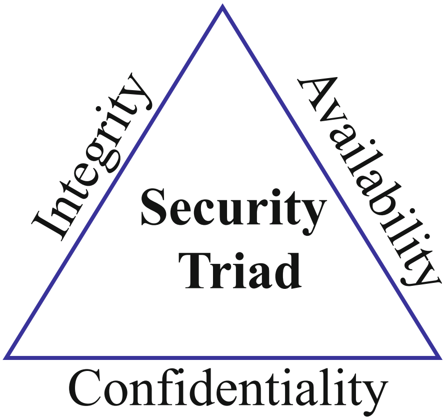
Fog computing incorporates three main components: IoT node, Fog node, and back-end cloud. It is vital to make the transmission secure between all these nodes. Existing privacy and security solution of cloud computing could be applied to some extent but still it has it's specific security challenges due to its features like decentralized infrastructure, mobility support, location awareness, and low latency. Therefore, new methods for securing Fog computing systems have been developed. In this chapter different security issues have been discussed for Fog computing in healthcare 4.0. Security challenges and their solutions have been proposed for each layer of Fog computing. This paper starts with an explanation of basic security issues—confidentiality, integrity, and availability. In addition, basic security architecture also has been discussed. Then different privacy and security threats are discussed based on the e-healthcare system. A pacemaker scenario of the implanted device is taken which illustrates the need for security and privacy in Fog-based IoT device. Different security issues from the perspective of the client, software, hardware, and physician have been discussed. Also, various attacks that can be performed on Fog devices or Fog networking have been discussed. The basic security architecture and network model define the traditional security scheme which states that it cannot be directly utilized for Fog computing. In this chapter Fog security challenges are classified into three sections: the first section introduces the network and service level security challenges, the second section covers the data center level challenges, and the last section covers the device level challenges.

12.2 Security Issues

12.2.1 CIA Triad (Confidentiality, Integrity, and Availability)

1. Confidentiality
   Confidentiality is about protecting private and sensitive information from unauthorized access. In healthcare Fog application securing data is the most important part. Also, data being sent over the Fog networks should not be accessed by unauthorized individuals. With the help of online available tools the attacker may try to capture these data and can gain access. The common ways to avoid this are to include access control, data and file encryption and system permissions (Fig. 12.1).
2. Integrity
   It is designed to protect data from modification or deletion from any unauthorized party. Patient's health-related information is most crucial for any health organization as the diagnosis is made out of such data. While transformation attacker can modify or delete or replay the information which causes a serious impact

Fig. 12.1 CIA triad



on patient's health and health organization too. The primary way to manage this issue is to make use of the hashing technique. There are various algorithms which implement hash function through which we can identify at receiver side that data has been modified or not.

3. Availability
   It is the last component of CIA triad which focuses on the vacancy of system or data when it is needed. Also, the network should be available whenever it is required. The motive behind this is to bring down services to compromise availability. DoS (Denial of Service) attack is an example of this component. The extra security equipment such as Firewall or proxy server can be used to safeguard the system.

12.2.2 Threats

Cloud Security Alliance has identified basic security issues. These issues directly impact onto different layers of Fog-enabled applications [2]. Depends on application security issues may vary. Some of the fundamental problems associated with Fog application in healthcare 4.0 are defined here.

1. Forgery
   Forgery is making fake identities or profiles to mislead end-users. This leads to fake information. Due to this in healthcare, it may lead to an unnecessary diagnosis or wrong prediction.
2. Tampering
   Tampering means modifying (destroying, manipulating, or editing) data by unauthorized users. An attacker may cause harm to the system or it may destroy data. An attacker can intercept the packet and can modify it. As patient's records

are most crucial in healthcare application, dropping or modifying the data may cause serious problems.

3. Sybil
   It is a peer-to-peer network threat in which a Fog node in the network operates multiple identities at the same time [3]. It gains the majority hold of Fog networks to carry out illegal actions. A single node can create and operate as multiple fake identities that affect the genuine user of the system.
4. Jamming
   Jamming jams the communication networks by spreading the bulk of dummy data on the network [4]. It may cause delay or destroying packets of system.
5. Eavesdropping
   Eavesdropping is a technique by which an unauthorized party captures the transmitting packets. It reads the pattern of transmission. This activity does not disrupt normal operation. Sender and receiver are completely unaware that data of the system is intercepted or stolen.
6. DoS (Denial of Service)
   This attack disrupts all the services of users by flooding unwanted requests to a victim node which blocks the route and does not allow to process legitimate requests.
7. Impersonation
   In this attacker pretends the fraud services as Fog services to the end-users. Attacker patiently examines all the fragments of information passing through an insecure medium or residing in the system. A combination of information gives the impersonator to fulfill their purpose. The more information they have, the better they can keep away from detection.

12.2.3 Privacy Issues

Privacy is an extreme problem in Fog computing for the healthcare system as the user's data is involved while collecting, storing, transmitting, and sharing through the medium. Privacy includes four facets, such as identity privacy, data privacy, usage privacy, and location privacy [5].

1. Identity privacy
   In this patient's personal information like name, address, telephone number, health record, disease, a public-key certificate may get a leak on a communication channel [6]. Here privacy of the user is not satisfied. While authentication when user's identities are submitted to Fog nodes it can be easily disclosed.
2. Data privacy
   It is an exposure of user data to unauthorized parties. It may be exposed while information are preserved on Fog nodes or transmitting among two parties. By examining these data attackers can get various information and these data may be used for illegal activities [6].

3. Location privacy
   There are so many massive applications available that collect user's location information. It captures the user's location records to reveal or have a look at the user's moments. It refers to the privacy of the user at the edge of the node. In the healthcare scenario patients or client uses many Fog services through which an attacker can easily know the route of information. Fog client chooses the nearest Fog server which is vulnerable to attacks. It can be preserved through various approaches like identity obstruction [7] as Fog node cannot directly identify the nearest Fog client. Different methods are there to apply this obstruction approach where a third party fake ID generator is used at each end-user. Instead of selecting the nearest location of Fog node it is selected primarily based on a few criteria like reputation, load balance, latency, etc. Due to this Fog node does not get an exact idea about the location of Fog client. But its location can be still traced by intersecting multiple nodes.
4. Usage privacy
   The user utilizes different services of Fog-enabled systems offered by Fog nodes. By compromising this issues attacker might also get utilization patterns of users with which a user makes use of services. For example, by analyzing services of e-health smart meter, users living patterns get disclosed like at what time they are at home, sleeping time, working hours, etc., which results in exposure of user's privacy.

12.2.4 Attacks

An attack is a procedure that involves an attempt to obtain, destroy, alter, remove, implant, or reveal information without having authorized rights. There are so many kinds of attacks emerging day by day. But mainly they are under either class of passive attacks or active attacks.

1. Wormhole attack
   Wormhole nodes make a fake path that is shorter than the original one within the network. This can confuse network routing mechanism and take the shortest fake path. This attack can be easily performed without knowing about the network topology.
2. Selective Forwarding
   Only the selective data packets are transmitted by an attacker and the rest of the packets are dropped [8]. It may lead to degradation of system performance.
3. Route Cache Poisoning
   It involves alteration of routing tables by malicious node. Packets are transmitted through the illegitimate path which leads to a alter or delete or removal of information.

4. Sybil
   It a kind of attack where nodes have a couple of identities over the network. These create confusion and disruption. This creates the chance for a malicious node to operate services of system [9].
5. Sinkhole
   In this malicious node pretends that this is an optimal route to reach the destination node [9]. This node sends fake messages to the initiator node, accordingly after receiving traffic, it alters the routing path. It complicates the topological structure of a network.
6. Hello Flood
   The attacker broadcast a link to all other nodes. An unaware node accepts that link and considers that this received node link is a neighbor node. Now, this unaware node transfers all packets that are actually received by the malicious node. This creates a routing loop within a network [9].
7. Byzantine
   In this, the attacker's aim is to decline network services. The attacker selectively drops packets which create routing loops and forward those packets to the non-optimal path.
8. Attacks Related to Data Privacy
   Generally, attackers are divided into three groups: cloud service providers, hackers, and governments. The cloud service provider has the bulk of the user's data. These data are gained by the service providers to make further analysis and improvement of mechanism. They are authorized to access these data as they have already taken terms and agreements. They use this data for marketing or share this data with another service provider. The agreements do not guarantee data confidentiality nor responsible for any misuse of data. The government can easily access the user's private data as they have legal permission to access. They can ask for such data from the service provider as they are the main source of data. These are meant for surveillance or analysis purpose for the benefit of citizens but if their data source is compromised, then any attacks can be easily performed. Hackers use such data for illegal activities.

12.2.5 Security Issues on the Basis of IoT Device of Healthcare

These security issues can be affected in many ways to healthcare Fog devices. Such issues can be illustrated through the example of pacemakers [10]. Pacemakers are medical devices which implanted in human bodies to monitor the human's heart rate. This device maintains the heart rate of the patient. Such devices fall under the category of healthcare 4.0 which needs the highest safety.

1. Clinical Perspective
   So many medical specialists are using such IoT devices to improve healthcare technology. These devices are implanted into many patients and they would not

believe without such a fully functional IoT device. Such patients need regular basis follow-up by doctor. The trained surgeon or medical practitioner performs program specific to the vendor which communicated with the device through wireless technology. There are technologies where this follow-up process can be made home-based, means patients do not have to come to the hospital on a regular basis, they can monitor from their respective location only. For that data, the module is needed which is located at the patient's location. Once implanted device fits into radio range of module, then contact is established and the nodes communicate with such devices. This information can be viewed by only authorized healthcare professionals.

The failure of such devices leads to a very high impact on human's life. Such failures lead to replacement. This arises high-security concerns in the device level unit. Such failure happened either by manufacturer defect or by an external entity. Remote follow-up can be monitored by an intruder who can perform attacks. Incorrect programming can occur either by error or technical failure or by malicious activity.

2. Risk Assessment
Security issues can be discussed according to CIA triad, which means confidentiality, integrity, and availability. Confidentiality states that data about the patient and the implanted device should be kept secure which could not be understood by any third party. Integrity means the data of IoT devices should not get alter as it results in high severe impacts on patients. Availability deals with the operability of the device. A pacemaker is a wireless device that communicates via the internet or LAN line or sometimes by USB stick. Overview of the pacemaker mechanism is shown in Fig. 12.2 [10].

Tampering or expose of information happens on any device. Like on the internet attack such as man in the middle attack can easily occur if proper

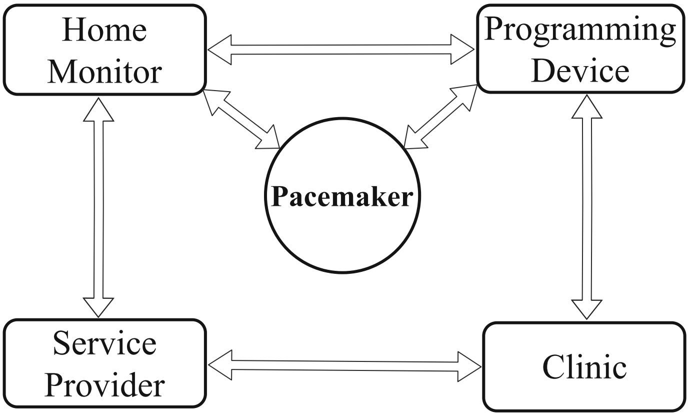


Fig. 12.2 General pacemaker scenario [10]

encryption mechanism is not used. The unsecured wireless medium can easily allow attackers to listen to traffic of network by any other malicious device. Such a malicious device acts as a legitimate user in a medium where DoS attacks also can be easily attempted.

3. Software
   Loopholes or bugs of software are used by a malicious intruder to gain access to the network. Software is uploaded into pacemaker as well as home monitor device and programming device. Software programming device helps to re-program a pacemaker, means it monitors the heart rate of the patient or can change pacemaker rate and processes data obtained from the pacemaker. This communicates with various models of devices. Like software of home, monitor communicates with a pacemaker and upload information regarding the patient to the server. This information can be later accessed by the physician. This needs regular periodic updates of software which minimizes loopholes of the system. If a programming device is compromised, then it may send the wrong parameter what actually being chosen while designing. Likewise, if home monitors are compromised, then it may upload wrong information to the server. This may lead to wrong analysis and computation that further harm the patient. A compromised server may possess such similar threats.
4. Hardware
   Hardware security is as needed as the software of any device. Various attacks like password stealing, login backdoor, privilege access are identified on the system. The various malicious circuits can be installed on the pacemaker as well as home monitoring devices. Malicious hardware mechanism can be installed on the server such as it can reveal or modify the sensitive data which mislead the doctor.
   Security challenges have been increased as such IoT devices have the capability of wireless communication. This includes unauthorized access as well as unauthorized modification of useful information. Device security is at most priority when the wireless network is used. Any intruder can change device configuration or disable any process or remotely run malicious command. The attacker uses compromised programming devices which allow them to access pacemaker and they pretend as a physician and get full rights to change parameters of such IoT device.

12.3 Security Challenges in Fog Computing for Healthcare 4.0

In healthcare applications, any assets like data records, sensors, devices are required to be protected. Compromised assets impact human phycology and can cause permanent loss. Fog IoT devices are resource constraints in terms of less memory, processing power, size limitations, a battery which leads to new level security

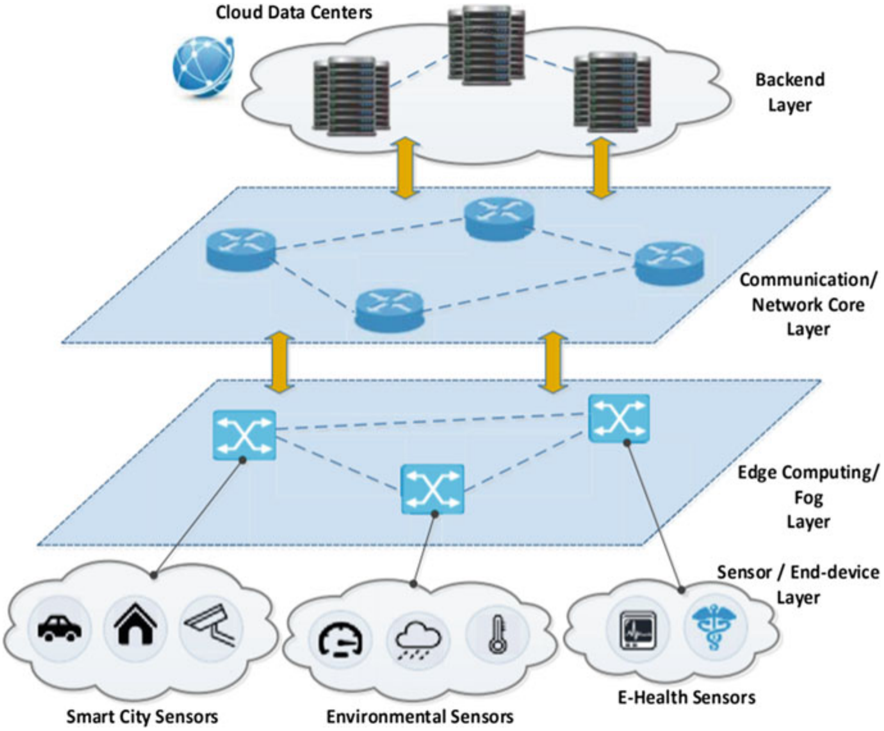


Fig. 12.3 Fog computing architecture [13]

challenges. Such medical devices must prevent unauthorized access but it should not reject legitimate user access at the time of emergency situations. A general security challenge for Fog computing is discussed as follows.

Fog-based architecture is more secure than cloud architecture. There are several reasons which forge more security challenges such as they are less dependent on the internet compared to cloud computing architecture, Fog nodes storage capacity is less complex than cloud and information exchange between the cloud [11]. Which emphasis more security challenges [11]. Fog-enabled system makes use of various networks for interconnecting different Fog nodes or devices such as mobile or wireless device network. This makes them potential targets for any attack [12]. As shown in Fig. 12.3 [13, 14], there are basically three layers of a Fog computing system. Each layer needs different security mechanisms than each other. Cloud computing security mechanism cannot be directly useful to each of these layers as each of the layers has different functionality. Therefore, the analysis of each layer is the most important.

Data centers contain all APIs that provide services to all other nodes which are part of Fog network and other process points like web applications for such reason data center have to be secure as patients' health is at great risk. Fog devices are also vulnerable for attacks as they actively communicate with each other.

Fog security challenges are divided into three classifications:

1. Network and service level security challenges
2. Datacenter level challenges
3. Device level challenges

12.3.1 Security Architecture

Security architecture is a unified secure model design that addresses the potential risk involved in certain scenarios. It specifies when and where to apply security protocols. It defines the relationship between components of a particular system. It is a standardized model, which makes it affordable. It provides different services which ensure that risk management, security policy, and standards, security architecture decision are in real-time applications. It incorporates security phenomena like threats, loopholes. The basic architecture to secure Fog computing mechanism is discussed below.

1. Network Security Model
   The two parties communicate with each other by establishing the path through the Internet between communicating nodes and by the cooperative use of communication protocols. Security becomes a basic need especially when it is desirable to protect the information transmission from an adversary who may introduce different threats.

   As shown in Fig. 12.4 [15], this model has basic four tasks as follows:

   1. Design an algorithm for security-related transmission. This algorithm should be such that the adversary should not gain control over the medium.
   2. Generate secret data used with the chosen algorithms.
   3. Introduce methods for the distribution of secret data.

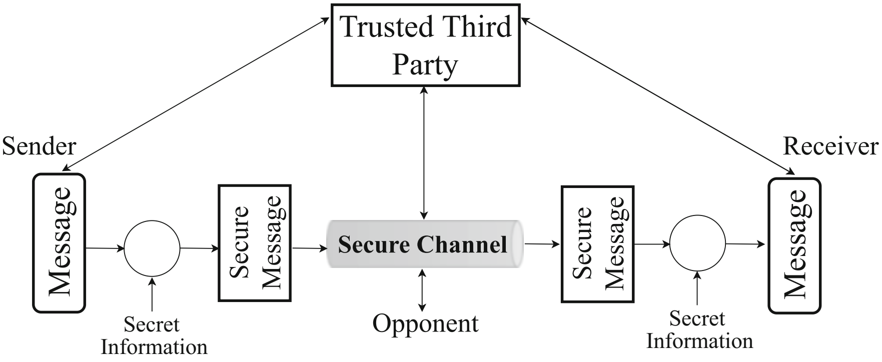


Fig. 12.4 Network security model [15]

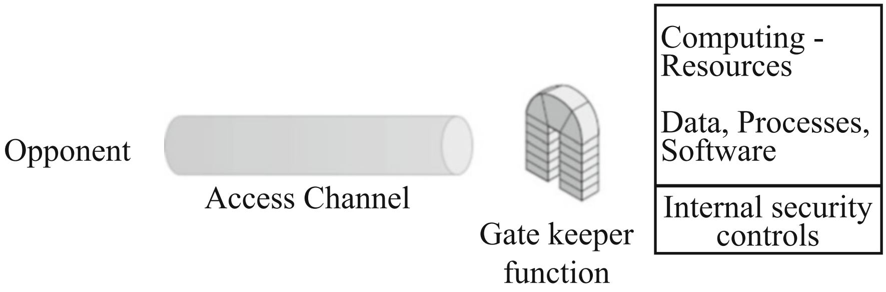


Fig. 12.5 Network access model [15]

4. Specify protocol used by two different parties which make use of the algorithm and secret information to achieve security services.

By achieving these four-task basic security needs can be fulfilled. There are so many different algorithms that are developed for security-related transmission which make use of secret information or key. This key should be as strong as possible as an intruder cannot deduce it. There are different methods for generating such keys. The same key can be used by two communicating parties or two different keys also can be used. Depending upon application two types of methods are used.

A trusted third party is needed for secure transmission. For example, it is responsible for distributing secret information, identify two communicating parties, or arbitrates disputes between the sender and receiver.

By advancing technology security requirements get changing. Other security-related issues are evolving that do not fit into this model. For example, different viruses, worm, hackers may penetrate as legitimate users and harm systems. A basic model for such different situations is illustrated in Fig. 12.5 [15]. Attacks can be introduced into a system that contains unwanted logic which can affect the system. The security mechanism is needed to cope up with such an attack as shown in Fig. 12.5. Gatekeeper authenticates the user. It includes two factor authentication procedures that are designed to deny access from unwanted users or activity. It detects the logic that contains unwanted activity such as malware, virus, worm and rejects another similar kind of attack. Once unwanted users or software gain access another kind of defense line is internal security control that monitors and detects any malicious activity.

12.4 Network and Service Level Challenges

Fog nodes have processing and storage capabilities. While processing and storage request devices interact with Fog nodes. Any other communication happens as a part of the Fog network [12]. Fog nodes interact with each other while managing network resources or the network itself. So, the following communication needs to be addressed to secure the Fog computing system:

1. Communication between devices and Fog nodes
2. Communication between Fog nodes

Fog nodes need to support different protocols such as ZigBee, Wi-Fi, 2G/3G/4G, WiMax, and so on [16]. While the cloud only supports TCP/IP. Fog-enabled system needs to maintain switch network between Fog nodes and cloud or between device and Fog nodes. While this shifting procedure security may compromise. This network needs to be secure by different security protocols.

Fog systems are deployed in a distributed environment. Each Fog server needs to manage a bunch of resources in a different location. Communication and synchronization between these nodes need to maintain security. If one of the Fog nodes is caught to be vulnerable by an attacker it can be compromised and the whole system's efficiency gets decreased. This will directly impact on patient's life at risk.

Data transmission between Fog node has many challenges. It needs to consider connection features. This means how the data get to travel through a medium is a need to specify either via a wireless medium or wired medium. An attacker can easily compromise these vulnerabilities if not properly secured as many tools are available to compromise such vulnerable medium [17].

There are several challenges that need to be addressed:

1. Authentication or identity verification
2. Access control
3. Protocol design
4. Intrusion detection
5. Trust management
6. Privacy-conserving packet forwarding
7. Rouge Fog node detection

12.4.1 Authentication or Identity Verification

Authentication or Identity verification checks for legitimate users or devices within the fog network to use fog-based application. There are many services offered by Fog-based systems. To use the services of Fog-enabled application users or devices must verify their identities in a secure manner. Without a sufficient security guarantee, it is easy for an attacker to target vulnerable services of resources. For example, an attacker may pretend as a valid user to access resources and would also not leave any evidence of their malicious activities. Therefore, authentication services need to be included.

So many authentication schemes are there to provide services to users like username and password, figure detection, or face detection [17, 18]. These schemes do not solve mobility issue of devices. In Fog computing user may travel from one region to another. They connect to different Fog nodes while traveling. If each Fog node performs authentication for accessing the services, then latency may get compromised. To solve this problem cooperative authentication schemes are used. It reduces the authentication overhead and authentication delay for individual users.

12.4.2 Access Control

Access control is the authorization process. Every user or IoT device has the right to access the services. But after gaining access to the system up to what level user or system can utilize the services is a part of the authorization. If there is no authorization architecture, then anyone can access anything and gain control over services and infrastructure. An attacker can easily penetrate into the system. Therefore, authorization mechanism has to be deployed. These include credentials for entities as well as various user factors like trustworthiness, occupation, resource ownership.

Currently, a role-based access control policy [19] is used widely to control access rights to network resources. It is based on the role of the user. Another policy used for authorization is attribute-based access control [20]. It is based on the user's certain attributes. If these attributes satisfy predefined attribute-based policy, then access permission can be granted. Fog computing is a distributed system where it is important to design a distributed access control mechanism. This should support the user's mobility and also device management [21] as a user can access services from any location with any kind of device because the user has multiple devices connected to the internet [22]. Also, the consistency of access policy should be maintained when the user makes use of different devices to access services.

12.4.3 Protocol Design

Real-time services are feasible in Fog computing because IoT devices communicate with Fog nodes in a very short range of communication. Delay of services just not depends only on bandwidth and communication range but also on processing delay of Fog nodes. If Fog nodes perform complex computational operations, then it generates more response delay. IoT devices do not have the capability to compute complex operations or cost too much time to execute them. Therefore, it is better to use lightweight protocol on both the side, IoT device and Fog nodes for performing computational operations.

A variety of security protocols are implemented to offer security and privacy on Fog nodes like authentication and authorization schemes, data encryption, spam detection, digital signature [23]. If they are not efficient enough, then the cost of computational resources increased. To overcome this lightweight cryptography is used. So many schemes have been developed like block ciphers, hash function, MAC (message authentication code), stream cipher to build an efficient and secure end-to-end communication between healthcare devices.

12.4.4 Intrusion Detection

The intrusion detection is introduced to discover malicious activity or policy violations of IoT and Fog nodes. Hole architecture of Fog computing needs to be protected by a defense mechanism. This makes the need to employ intrusion detection for Fog node and IoT devices. Based on the need for security different types of intrusion detection mechanisms like host-based or network-based IDS are used.

A host-based IDS runs on the system and monitors it. For example, it examines system logs, typical fail login, or installation of a back door. For each object IDS keep track of specific attributes like permissions, modification dates, checksum, or size to recognize changes.

Network-based IDS monitors network packets. It examines signs of reconnaissance, DoS attacks malware or viruses, traffic of population of the host, patterns shared between clients. It is useful to detect any attack that is able to penetrate successfully to the Fog computing system. Bayesian network classifier and threat protocol have been developed which provide reliable communication and anomaly detection [24]. This approach is more effective for efficient monitoring compared to traditional cloud based system.

12.4.5 Trust Management

Authentication and access control are not enough to get rid of fake Fog nodes or devices as it is still not guaranteed that all the joining nodes are fully trusted. A Fog node may not blindly trust to neighbor nodes as they may get infected by intruder.

Two basic trust models have been used widely: evidence-based trust model and monitoring based trust model [25]. In evidence-based, there is evidence that proves the trust relationship of Fog nodes like a public key, identity, or any evidence that the user has to prove there trustworthiness. Traditional cryptography was part of an evidence-based trust management scheme. Monitor based trust management is achieved by observing nodes' behavior and its past experience and responses. This trust model can be evaluated by direct evidence or indirect evidence. In direct evidence, trust value is evaluated by examining dropping packets and modifying packets. Forwarded packets are observed with the original packets to identify malicious behavior.

12.4.6 Privacy in Packet Forwarding

Privacy of every packets which are coming from various devices needs to be consistent and private as they carry crucial information. The leakage of privacy should not be compromised as clinical records of any individual play an important role while processing and evaluating.

Many solutions are available to secure packet forwarding like remote data integrity verification, which verifies data integrity. The basic security solution is data encryption before uploading on the network. An atomic proxy cryptography was proposed in which a semi-trusted proxy converts ciphertext without watching the original message using proxy encryption key [26]. Blind signature based secured e-healthcare system has been developed which maintains patient privacy [27]. The main components which are focused in this system are identity, privacy anonymity, and credentials [27].

12.4.7 Rough Fog Node Detection

In Fog computing environment workload is divided into several Fog nodes. This increases efficiency and response time. A Fog node is said to be a rough node when malicious Fog node pretends to be a legitimate node; hence, maintaining data integrity is necessary. Therefore, before any data processing and computation start it is necessary to establish trust management. This requires an authentication protocol.

12.5 Data Center Level Challenges

Data can be collected from various IoT devices and stored at Fog nodes temporarily. Because of this, the data can be readily available for frequent access. This helps to maintain and organize data easily. Data are temporary stored in the Fog nodes. The Fog has different capabilities of data collection, assembling, routing, packet forwarding [28]. It is also capable of simple processing of data and selects the appropriate one depending on the application. Fog node data centers cooperate with each other and also connected with the cloud. It is very important to safeguard data collection and distribution as especially when the health of individuals is a concern [29]. SDN (Software Design Network) is a new latest technology used in data center level that provides centralized control [30]. Large number of data is produced from different sources such as healthcare, financial companies, Internet, etc. [31]. For real-time analysis and to incorporate dimensionality reduction of Big data system PCA (principal component analysis) and SVD (singular value decomposition) are used [32]. There are several challenges which are to be considered at the data center level:

1. Data identification, aggregation, and integrity
2. Secure content distribution
3. Verifiable computation
4. Secure computation

12.5.1 Data Identification, Aggregation, and Integrity

A massive quantity of records have been generated by IoT devices but not all data are useful or meant to be stored on Fog nodes. Before uploading data to the data center their identification, aggregation, and integrity are highly important. Also temporarily maintained data is required to minimize management complexity. Privacy is the utmost need which affects data confidentiality, integrity, and sharing. Distinguishing sensitive information from data is an important task for Fog mechanism. There is mechanism that identifies malicious downloaded data which is based on a blacklist of malicious file hashes [33].

Fog nodes are able to process, modify, and delete useless data and forward it to the cloud. Therefore, determining the honesty of Fog node is difficult. Also due to mobility features, multiple Fog nodes may have user's data. So, to satisfy the integrity of data many possession protocols have been proposed [34, 35]. These protocols guarantee integrity and correctness of data.

Each device collects data from different sources and encrypts it to preserve data privacy. After encryption, it is forwarded to Fog nodes. Then Fog node stores these data depending on the requirement and delivers it to the cloud. During this process, secure data aggregation is crucial to prevent data leakage.

12.5.2 Secure Content Distribution

Secure transferring of data is a basic requirement in Fog computing healthcare. For example, records gathered by IoT devices which are fit into the human body should be shared with family doctors. Sharing of such records with other nodes or devices is a challenging task. For secure transfer, several cryptography schemes have been widely used like proxy re-encryption [36], attribute-based encryption, key aggregate encryption.

Attribute encryption can be used for data security and sharing. In this user's key and ciphertext depend upon attributes. Several schemes have been developed, which can be divided into two parts: key-policy attribute-based encryption [37] and cipher-policy attribute-based encryption [38].

The key aggregate scheme satisfies efficient and secure data sharing through compact keys. The size of the key is independent of ciphertext, no matter how many numbers of ciphertext upload on the server.

12.5.3 Verifiable Computation

Fog computing has computation resources designed for specific computational tasks that produce a result with low latency. This result cannot be fully trusted. This makes a huge concern for the user's as their device does not have that much computation capability to verify it [39]. Cloud has also been connected with Fog nodes in a distributed environment. So correctness verification of result is necessary for users as well as cloud. If there is no mechanism to check the correctness, then the user may not use services offered by Fog nodes.

So many various schemes have been applied to check the correctness of the result. Yao's Garbled Circuits [40, 41] describe a non-interactive outsourcing verifiable computation scheme with fully homomorphic encryption (method of encryption which allows data to be in the encrypted form while it is being analyzed and processed.). Attributes based encryption verifiable computation scheme has been proposed which concerned with the design of public verifiable computation protocol.

12.5.4 Secure Computation

Fog computing is a distributed environment where user's do not have full control over computations. IoT devices expose all collected sensitive information to Fog node and then it executes computation which generates privacy and security concerns. Moreover, if secret key is exposed, then node may pretend as a legitimate user and do everything they want.

Numerous server-aided computations are introduced [42, 43]. Their motto is to reduce the computational time and to keep the records secret from the server. The server-aided verification concept has been introduced which speeds up the verification step of an authentication/signature mechanism [44]. In this method for designing SAV different schemes have been proposed [44]. The security model for a server-aided verification signature has been introduced through which verification of signatures can be performed with less computational cost compared to the original computational algorithm [45]. Moreover, other additional server-aided schemes have been proposed like server-aided encryption [46], server-aided function evaluation [47], server-aided key exchange [48] to speed up computations for users.

12.6 Device Level Challenges

In the Fog computing system, each device has a unique identity, visibility, and task. Not all devices are capable of handling the whole system architecture. All systems of Fog computing are assigned with a specified constraint like computational capabilities, limited power, storage [49]. Thus, Fog nodes send data to the upper layer through gateways for further processing. The system of any environment brings significant privacy and security concerns [50]. The following issues must be considered for securing data at the device level.

1. Confidentiality
2. Lightweight trust management

12.6.1 Confidentiality

System confidentiality means protecting resources from unauthorized access and safeguard data. Existing PKI based system has heavyweight computation and storage. Therefore, it is not effective to apply existing solutions to a Fog-based environment. These solutions are useful in terms of fixed large key size which requires more memory and processing power. They also do not protect systems from insider attacks. Authentication and privacy are basic security requirements for Fog system environments.

1. Authentication
   Fog computing services are offered to huge number of end users via Fog nodes [51]. User-friendly and secure solutions exist to solve authentication issues [50, 51]. In addition, biometric authentication is the most needed technology specifically in the environment of mobile computing, Fog computing [52]. Touch base authentication, fingerprint authentication, face authentication are widely used in this technique [53].
2. Privacy
   Users are more concerned about their private and sensitive information such as personal data, location, or other information while using cloud or Fog based services [51]. IoT user's identities must be protected from getting exposed to the adversary. Group signature or connection anonymization techniques are developed for preserving identity privacy [54]. Fog node collects security data from IoT devices and sensors. Homomorphic or differential privacy can be employed to ensure the privacy of uniform data entries [55]. Several techniques are proposed to obfuscate identity [56]. Different methods are evolving to secure the privacy of the client's location [57].

12.6.2 Lightweight Trust Management

The Fog-based IoT devices should have a certain trust level among them. Authentication plays a crucial role to build trust between Fog-based system. Traditional trust-based routing protocols have different issues like more memory and power consumption [51]. Therefore, there is a need to design a lightweight trust mechanism. Such systems are more effective in identifying malicious nodes or devices [57].

12.6.3 Blockchain Approach

Blockchain is a distributed and decentralized technology which comprises various techniques and services like hash cryptography, immutable ledger, consensus protocol, and P2P networking and mining [58]. It provides great security and privacy in an easy, efficient, and secure manner. It is also implemented as an authorized identity of IoT devices. Its decentralized feature provides great security, authentication, and integrity of data which is communicated between two Fog nodes or between two clients or patients in a confidential manner. Through this technique secure tracking of IoT device transactions made easy.

Blockchain has another feature to deal with authorization of IoT device which provides effective rules for authentication which has less complexity compared to conventional protocol. In this approach, there is no need for third party and still they can securely communicate and perform the execution. Blockchain provides unique GUID and symmetric key pairs to each device of Fog computing which removes key distribution and management process [51]. We can increase the feasibility of lightweight protocol by using this approach as Fog computing has constrained computational and storage capacity. It provides secure communication among different Fog nodes and between layers of Fog computing. It authenticates the identity of the user and ensures the transaction made by the authentic user. It also ensures verifies transaction made by the authentic users. The greatest advantage is there is no single point of failure as copy of records is stored on every device.

There are a few challenges associated with this approach. In Fog computing technology adaptive and lightweight blockchain security solution is needed as it has less storage capacity and computational power. Bitcoin blockchain has latency in terms of latency; therefore, it is not feasible to use bitcoin approach in real-time.

Blockchain and Fog Computing IoT

Fog-based IoT system has great security and privacy issues. A huge number of data or information is produced by interconnected IoT devices which have to be kept confidential. End-to-end security and trust have to be built up. Implementation of blockchain can overcome such problems. Fog computing has a distributed trust and security solution; therefore to build and manage with such solutions, Fog computing uses the blockchain approach [51]. To provide fast services in medical industry FAAL based structure also has been proposed which uses the distributed concept for networking and storage [59]. When a new device is connected to Fog computing system, blockchain architecture provides security to the whole network. It also detects and isolates malicious or compromised node. This provides self-identification and solution of the problems. Data is at the highest priority level in any healthcare IoT system. This technique removes third party intervention. In this regard, blockchain provides the highest security solution. It provides secure storage and transmission through digital signature for more protection and privacy [51]. Also, this can directly transfer data among devices through a time-stamp based method with proper security [60].

To improve system performance and capacity a distributed IoT network architecture consisting of an SDN based network using the blockchain technique is developed [61]. It provides threat prevention, access control, data protection, and other attacks such as ARP spoofing or DDoS (Distributed Denial of service)/DoS(Denial of Service) attack. For authentication, a decentralized authentication mechanism based on a public blockchain is developed which creates a secure virtual zone for secure communication [62]. In healthcare domain records of patient's are crucial as any small change to it puts into a big trouble. To secure such records blockchain based method can be used in which patient has whole control and rights over his records so as to monitor all transactions [63].

A lightweight FC-based hierarchical architecture for IoT is developed that has secure trust management which reduces block management processing time. It provides the solution of lightweight Fog IoT devices with better security privacy. It eliminates overhead with conventional blockchain. A blockchain-based decentralized, infrastructure-independent technique [51] has been developed for securing a patient's or client's location and privacy [64]. It stresses proofs of location, verifies geographic location, and preserves user location privacy. Healthcare data gateway (HDG) is a blockchain-based scheme that is developed to enable the patient to communicate easily and securely [65]. For any financial transaction also this approach provides more security. BloHost framework is proposed for transaction through single unified cryptocurrency [66].

Practical implementation of blockchain based approach has several challenges [67]. Blockchain is replaced with client–server system technology. But FC-based information required less memory and power. Also, increase in number of nodes may degrade the performance of blockchain architecture [68].

12.7 Conclusion

Fog-based IoT devices are prone to different security attacks due to lack of constraint resources and security design of hardware or software. In the healthcare domain technology of Fog computing is widely developing. But securing such medical devices leads to securing human life, health, and well-being. It also includes the protection of health-related information and secures the privacy of those data. Increasing use of the mobile medical application and medical devices that use wireless communication requires a high-security mechanism. In this chapter potential security and privacy challenges for Fog computing in healthcare 4.0 have been discussed. Various security and privacy issues along with their solutions have been discussed. The basic security mechanism is illustrated to state that existing security solutions cannot be directly applied to Fog computing. The medical scenario has been taken to illustrate the challenges and vulnerabilities of the use of Fog-enabled devices in medical applications. New emerging technologies for healthcare application provide an opportunity with security to make the medical field more cost-effective and user beneficial for human well-being. If proper countermeasures are not taken to secure Fog-based IoT device, then misuse of medical data and malware attacks are easy to perform which puts human life in danger.

References

1. Sangita, D., Ankita, C., & Reshamlal, P. (2015). A review on issues and challenges of cloud computing. *International Journal of Innovations and Advancement in Computer Science, 4*(1), 81–88.
2. Top Threats Working Group. (2016). *The treacherous 12: cloud computing top threats in 2016*. Seattle: Cloud Security Alliance.
3. Mishra, A. K., Tripathy, A. K., Puthal, D., & Yang, L. T. (2018). Analytical model for Sybil attack phases in internet of things. *IEEE Internet of Things Journal, 6*(1), 379–387.
4. Fadele, A. A., Othman, M., Hashem, I. A. T., Yaqoob, I., Imran, M., & Shoaib, M. (2019). A novel countermeasure technique for reactive jamming attack in internet of things. *Multimedia Tools and Applications, 78*(21), 29899–29920.
5. Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Fog computing for Healthcare 4.0 environment: Opportunities and challenges. *Computers & Electrical Engineering, 72*, 1–13.
6. Lin, X, Ni, J., & Shen, X. (2018). *Privacy-enhancing fog computing and its applications*. Basel: Springer International Publishing.
7. Kumar, P., Zaidi, N., & Choudhury, T. (2016). Fog computing: Common security issues and proposed countermeasures. In *2016 International Conference System Modeling & Advancement in Research Trends (SMART)* (pp. 311–315). Piscataway: IEEE.
8. Huang, C., Liu, D., Ni, J., Lu, R., & Shen, X. (2018). Reliable and privacy-preserving selective data aggregation for fog-based IoT. In *2018 IEEE International Conference on Communications (ICC)* (pp. 1–6). Piscataway: IEEE.
9. Tanwar, S., Thakkar, K., Thakor, R., & Singh, P. K. (2018). M-Tesla-based security assessment in wireless sensor network. *Procedia Computer Science, 132*, 1154–1162.
10. Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM, 58*(4), 74–82.
11. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing, 21*(2), 34–42.
12. Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., et al. (2017). Security and privacy in fog computing: Challenges. *IEEE Access, 5*, 19293–19304.
13. Khan, S., Parkinson, S., & Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. *Journal of Cloud Computing, 6*(1), 19.
14. Atlam, H., Walters, R., Wills, G. (2018). Fog computing and the internet of things: a review. *Big Data and Cognitive Computing, 2*(2), 10.

15. Stallings, W. (2006) Cryptography and network security, 4/E. Pearson Education India.
16. Shi, Y., Ding, G., Wang, H., Eduardo Roman, H., & Lu, S. (2015). The fog computing service for healthcare. In *2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (Ubi-HealthTech)* (pp. 1–5). Piscataway: IEEE.
17. Lee, K., Kim, D., Ha, D., Rajput, U., & Oh, H. (2015). On security and privacy issues of fog computing supported Internet of Things environment. In *2015 6th International Conference on the Network of the Future (NOF)* (pp. 1–3). Piscataway: IEEE.
18. Li, C., Qin, Z., Novak, E., & Li, Q. (2017). Securing SDN infrastructure of IoT–fog networks from MitM attacks. *IEEE Internet of Things Journal, 4*(5), 1156–1164.
19. Salonikias, S., Mavridis, I., & Gritzalis, D. (2015). Access control issues in utilizing fog computing for transport infrastructure. In *International Conference on Critical Information Infrastructures Security* (pp. 15–26). Cham: Springer.
20. Lewko, A., & Waters, B. (2011). Decentralizing attribute-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 568–588). Berlin: Springer.
21. Steiner, P. (2014). Going beyond mobile device management. *Computer Fraud & Security, 2014*(4), 19–20.
22. Ni, J., Lin, X., Zhang, K., Yu, Y., & Shen, X. S. (2016). Device-invisible two-factor authenticated key agreement protocol for BYOD. In *2016 IEEE/CIC International Conference on Communications in China (ICCC)* (pp. 1–6). Piscataway: IEEE.
23. Vora, J., Italiya, P., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., et al. (2018). Ensuring privacy and security in E-health records. In *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 1–5). Piscataway: IEEE.
24. Tanwar, S., Vora, J., Kaneriya, S., Tyagi, S., Kumar, N., Sharma, V., et al. (2019). Human arthritis analysis in fog computing environment using Bayesian network classifier and thread protocol. *IEEE Consumer Electronics Magazine, 9*(1), 88–94.
25. Cho, J.-H., Swami, A., & Chen, R. (2010). A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys & Tutorials, 13*(4), 562–583.
26. Hou, J., Jiang, M., Guo, Y., & Song, W. (2019). Efficient identity-based multi-bit proxy re-encryption over lattice in the standard model. *Journal of Information Security and Applications, 47*, 329–334.
27. Vora, J., DevMurari, P., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2018). Blind signatures based secured e-healthcare system. In *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 1–5). Piscataway: IEEE.
28. Kumari, A., Tanwar, S., Tyagi, S., Kumar, N., Parizi, R. M., & Choo, K.-K. R. (2019). Fog data analytics: A taxonomy and process model. *Journal of Network and Computer Applications, 128*, 90–104.
29. Vora, J., Italiya, P., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., et al. (2018). Ensuring privacy and security in E-health records. In *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)* (pp. 1–5). Piscataway: IEEE.
30. Vora, J., Kaneriya, S., Tanwar, S., & Tyagi, S. (2018). Performance evaluation of SDN based virtualization for data center networks. In *2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1–5). Piscataway: IEEE.
31. Kumari, A., Tanwar, S., Tyagi, S., Kumar, N., Maasberg, M., & Choo, K.-K. R. (2018). Multimedia big data computing and Internet of Things applications: A taxonomy and process model. *Journal of Network and Computer Applications, 124*, 169–195.
32. Tanwar, S., Ramani, T., & Tyagi, S. (2017). Dimensionality reduction using PCA and SVD in big data: A comparative case study. In *International Conference on Future Internet Technologies and Trends* (pp. 116–125). Cham: Springer.
33. Ghafir, I., & Prenosil, V. (2016). Malicious file hash detection and drive-by download attacks. In *Proceedings of the Second International Conference on Computer and Communication Technologies* (pp. 661–669). New Delhi: Springer.

34. Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., et al. (2016). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. *IEEE Transactions on Information Forensics and Security, 12*(4), 767–778.
35. Zhu, Y., Hu, H., Ahn, G.-J., & Yu, M. (2012). Cooperative provable data possession for integrity verification in multicloud storage. *IEEE Transactions on Parallel and Distributed Systems, 23*(12), 2231–2244.
36. Blaze, M., Bleumer, G., & Strauss, M. (1998). Divertible protocols and atomic proxy cryptography. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 127–144). Berlin: Springer.
37. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM Conference on Computer and Communications Security* (pp. 89–98). New York: ACM.
38. Bethencourt, J., Sahai, A., & Waters. B. (2007). Ciphertext-policy attribute-based encryption. In *2007 IEEE symposium on security and privacy (SP'07)* (pp. 321–334). Piscataway: IEEE.
39. Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Verification and validation techniques for streaming big data analytics in internet of things environment. *IET Networks, 8*(2), 92–100.
40. Gennaro, R., Gentry, C., & Parno, B. (2010). Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In *Annual Cryptology Conference* (pp. 465–482). Berlin: Springer.
41. Chung, K.-M., Kalai, Y., & Vadhan, S. (2010). Improved delegation of computation using fully homomorphic encryption. In *Annual Cryptology Conference* (pp. 483–501). Berlin: Springer.
42. Kawamura, S.-i., & Shimbo, A. (1993). Fast server-aided secret computation protocols for modular exponentiation. *IEEE Journal on Selected Areas in Communications, 11*(5), 778–784.
43. Cavallo, B., Di Crescenzo, G., Kahrobaei, D., & Shpilrain, V. (2015). Efficient and secure delegation of group exponentiation to a single server. In *International workshop on radio frequency identification: security and privacy issues* (pp. 156–173). Cham: Springer.
44. Girault, M., & Lefranc, D. (2005). Server-aided verification: theory and practice. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 605–623). Berlin: Springer.
45. Wu, W., Mu, Y., Susilo, W., & Huang, X. (2008). Server-aided verification signatures: Definitions and new constructions. In *International Conference on Provable Security* (pp. 141–155). Berlin: Springer.
46. Rao, N. S., & Gopi Krishna, V. (2016). Data integrity auditing and secure deduplication on cloud using secure systems. *International Journal of Scientific Research in Science, Engineering and Technology, 2*(6), 175–187.
47. Kamara, S., Mohassel, P., & Riva, B. (2012). Salus: A system for server-aided secure function evaluation. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (pp. 797–808). New York: ACM.
48. Cliff, Y., Tin, Y. S. T., & Boyd, C. (2006). Password based server aided key exchange. In *International Conference on Applied Cryptography and Network Security* (pp. 146–161). Berlin: Springer.
49. Vora, J., Kaneriya, S., Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2019). TILAA: Tactile internet-based ambient assistant living in fog environment. *Future Generation Computer Systems, 98*, 635–649.
50. Balfanz, D., Smetters, D. K., Stewart, P., & Chi Wong, H. (2002). Talking to strangers: authentication in ad-hoc wireless networks. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2002*.
51. Tariq, N., Asim, M., Al-Obeidat, F., Farooqi, M. Z., Baker, T., Hammoudeh, M., et al. (2019). The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors, 19*(8), 1788.
52. Hathaliya, J. J., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Securing electronics healthcare records in Healthcare 4.0: A biometric-based approach. *Computers & Electrical Engineering, 76*, 398–410.

53. Hathaliya, J. J., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Securing electronics healthcare records in Healthcare 4.0: a biometric-based approach. *Computers & Electrical Engineering, 76*, 398–410.
54. Sen, J. (2010). Privacy preservation technologies in Internet of Things. Preprint. arXiv:1012.2177.
55. Van Tilborg, H. C. A., & Jajodia, S. (Eds). (2014). *Encyclopedia of cryptography and security*. Berlin: Springer Science & Business Media.
56. Wei, W., Xu, F., & Li, Q. (2012). MobiShare: Flexible privacy-preserving location sharing in mobile online social networks. In *2012 Proceedings IEEE INFOCOM* (pp. 2616–2620). Piscataway: IEEE.
57. Gong, P., Chen, T. M., & Xu, Q. (2015). ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks. *Journal of Sensors, 2015*, 1–10.
58. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications, 50*, 102407.
59. Vora, J., Tanwar, S., Tyagi, S., Kumar, N., & Rodrigues, J. (2017). FAAL: Fog computing-based patient monitoring system for ambient assisted living. In *2017 IEEE 19th International Conference on E-Health Networking, Applications and Services (Healthcom)*. Piscataway: IEEE.
60. Li, M., Zhu, L., & Lin, X. (2018). Efficient and privacy-preserving carpooling using blockchain-assisted vehicular Fog computing. *IEEE Internet of Things Journal, 6*(3), 4573–4584.
61. Sharma, P. K., Singh, S., Jeong, Y.-S., & Park, J. H. (2017). DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks. *IEEE Communications Magazine, 55*(9), 78–85.
62. Hammi, M. T., Hammi, B., Bellot, P., Serhrouchni, A. (2018). Bubbles of Trust: a decentralized blockchain-based authentication system for IoT. *Computers & Security, 78*, 126–142.
63. Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., et al. (2018). BHEEM: A blockchain-based framework for securing electronic health records. In *2018 IEEE GLOBECOM Workshops (GC Wkshps)*. Piscataway: IEEE.
64. Brambilla, G., Amoretti, M., & Zanichelli, F. (2016). Using blockchain for peer-to-peer proof-of-location. Preprint. arXiv:1607.00174.
65. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems, 40*(10): 218.
66. Bodkhe, U., Bhattacharya, P., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S. (2019). BloHost: Blockchain enabled smart tourism and hospitality management. In *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*. Piscataway: IEEE.
67. Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mechanical Systems and Signal Processing, 135*, 106382.
68. Tanwar, S., Parekh, K., Evans, R. (2019). Blockchain-based electronic healthcare record system for Healthcare 4.0 applications. *Journal of Information Security and Applications, 50*, 1–14.