How to Cite:
Sharma, N., Bansal, L., & Prabha, C. (2022). Security and protection in fog computing: A review. *International Journal of Health Sciences*, *6*(S8), 5199–5211. Retrieved from https://sciencescholar.us/journal/index.php/ijhs/article/view/13423

Security and protection in fog computing: A review

Neha Sharma
Assistant Professor, Department ofComputer science and Engineering, CGC Landran and Research Scholar, Department of Computer science and Engineering, Chandigarh University, Punjab, India
Corresponding author email: lovishbansal55@gmail.com

Lovish Bansal
Student (B.Tech), Department of Computer science and Engineering, CGC Landran, Punjab, India
Email: neha.4815@cgc.edu.in

Chander Prabha
Professor, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India
Email: prabhanice@gmail.com

***Abstract*---**Rapid innovations in the fields of cloud computing in mobile phones, cloudlets, etc and fog and edge computing are a reason why IoT (Internet of Things) devices have seen a rapid surge. There are several limitations in the cloud computing paradigm such as bandwidth, location awareness, latency, constraints of resources and several other factors. To address these challenges, the term "fog computing" was coined. Here we discuss the layout and structure of fog paradigm which is followed by broadly analysing the characteristics of fog computing structure. Finally the paper is concluded by discussing security challenges and solutions in fog computing.

***Keywords*---**internet of things, fog computing, cloud computing, privacy, security.

Introduction

In today's world data is generated at a large scale consistently [1]. Many organizations depend on cloud computing provided by cloud servers for the storage of the data generated by them as cloud storage helps companies and its users to store their data in the cloud instead of local systems which can then be

accessed through network connectivity [2]. Though cloud provides a lot of advantages but with the continuous expansion of devices using internet it is set to generate data storage problems and increase latency. To solve the limitations of cloud computing related to the storage of data and increased latency the concept of fog computing was presented [3]. Fog computing helps provide low latency, thus improving quality of service (QoS) provided in real-time applications and environments [4]. Fog computing moves ahead from the centralized model used by cloud and instead provides a distributed model by providing various cloud services like computation, storage, etc at the corner of our network [5]. As fog is like a cloud closer to the surface, similarly fog paradigm puts storage and processing closer to the final user [4]. The infrastructure for fog computing connects various fog nodes together situated at the end of the network in a spread out manner to improve elasticity, redundancy and scalability [6]. Fog computing interconnects end devices and cloud by introducing fog nodes between them to perform computations more accurately and quickly. As an example before data is passed on to the cloud it is aggregated and filtered in the fog nodes [4]. Fog computation finds major implementation in IoT. Its characteristics like mobility support, heterogeneity, low latency, real time applications, geographical allocation and decentralized data expository, etc. fog computing serves as a better fitting place for executing the internet of things devices [3, 4, 5]. Fog computing helps transfer various new information for computing devices by acting as a link between the final devices and the cloud. Various devices such as access points, set top boxes, and proxy servers act as the computing devices called fog nodes [4]. In the internet of things fog computing aids in cutting down the information passing to cloud for storing and analysis, instead, the data collected by the devices with sensors is passed to the network appliances like edge for processing and storing it temporarily, which in turn reduces the latency and network load helping the devices using IoT to process data quickly. For this various smart devices such as switches, smart phones, routers, etc. are made to perform as fog computing devices by the installation of storage and computing power [1]. When data is generated or needed by an end device the cloud center is usually located far from it and for end device to directly communicate with it several network hops are required which creates a lot of overhead, which can cause problems for applications like gaming, road traffic lights and augmented reality. As end devices keep increasing a large chunk of information is shifted to the cloud creating a lot of network traffic causing congestion. This problem gets solved by the fog nodes introduced among the cloud layer and the end layer by fog computing. The combination of the cloud server, the fog nodes and the end devices working together fog computing effectively provides latency- critical applications [7]. The various architectural models of fog computing are based on three layered structure comprising of device layer or terminal layer as its first layer, fog layer as the second layer and cloud layer as the third layer [3,4,5,7]. These layers are all present in a hierarchal form as shown in the figure 1.

Device layer

Device layer is the layer closest to real environment. It is composed of several IoT devices like smart phones, smart cards, mobile phones, smart vehicles, etc., distributed geographically. They act as computing gadgets and detect information

from various physical objects which is then transferred to the fog layer for further analysing and handling of storage [3, 4].

Fog layer

This layer exists among the cloud and IoT devices and it helps in the communication among the cloud layer and the layer of end devices. It consists of network devices like switches, access points, routers, gateways, etc., that act as fog servers. Fog servers are responsible from the collection of information from end devices. They also process the data and store it temporarily. These fog devices are easily associable by the edge devices. Due to their ability to perform real-time analyses, latency information is adaptable in the fog layer. The fog layer consists of fog nodes that are computational centers present near the network edge. Fog nodes are like small data storing centers present close to corner of the internetwork and used by various end devices present around it. The end devices send various computational tasks to any fog node present near it. Using these decentralized fog nodes instead of clouds leads to reduction in latency and reduces network traffic. The fog nodes can be devices put specially for acting as fog nodes or existing network devices furnished with extra storage and computational capacity. As the fog nodes are usually just 1-2 hops away from end devices they reduce latency as compared to cloud which usually require a lot more hops [3,4, 7].

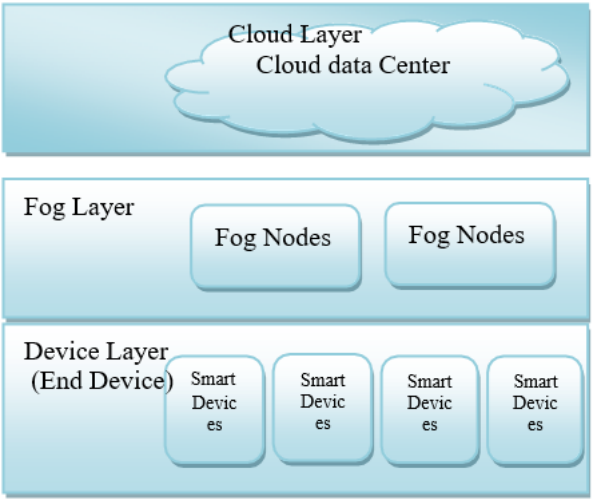

Fig. 1 Architecture of fog computing [4].

Cloud layer

The uppermost layer in fog paradigm architecture is the cloud layer. It has cloud intelligence and has the ability to store and process a huge amount of information. The amount of data that can be processed is dependent on the capability of a information centre which handles duty for doing all the decisions regarding storage and processing of information. Part of this task is assigned to the fog nodes to improve transmission efficiency. These fog nodes have limited capacity while cloud has a larger capacity though they are less in number. The

data from fog nodes is transferred to cloud from time to time whenever required for fixed storage. Data transfer to cloud involves higher latency, so addition of fog layer in the end devices and the cloud layer reduces latency and working of these three layers makes data transfer very efficient [4,7].

Fog computing characteristics

Paradigm of fog computing places services closer to end user, making it more advantageous as compared to other computing paradigms. The various essential characteristics that distinguish fog computing from other paradigms are shown in figure 2 [8].

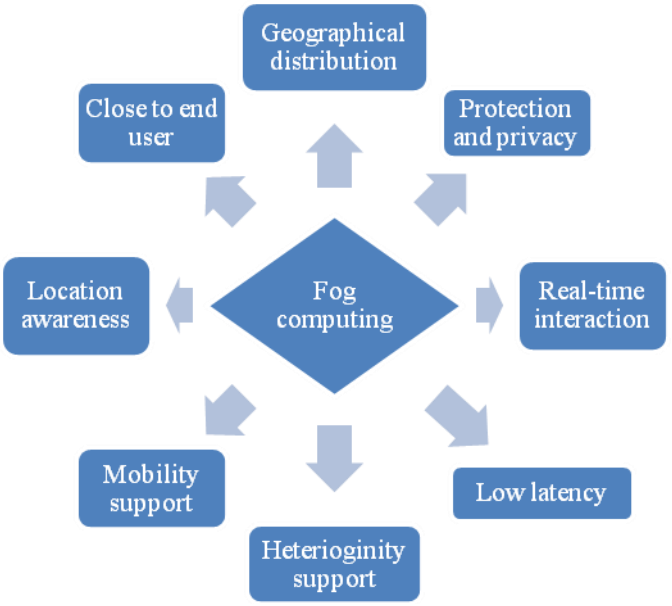

Fig. 2 Characteristics of fog computing[11]

Geographical distribution: Fog computing helps to distribute nodes in several different geographical locations [9]. As opposed to cloud that uses centralized model, services and applications of fog like IoT require widely distributed deployment of fog nodes in geographically identifiable locations. Fog computing can help in providing high quality data streaming for high speed vehicles with the use of proxies or access points present along highways [10]. Fog delivers high quality streaming services as it works in a distributed environment [11].

Proximity to end users: Fog computing rearrange fog devices in a particular area and analyses local content in order to provide high rate services locally usually based on the locations of fog devices. For example if the location of a mobile user is in a shopping mall, his service demands are more predictable as he would be more interested in local sales, cafes, etc. This is enabled by fog computing [10]. Location Awareness: The power of gaining knowledge of the geographical position of any device is known as location awareness. In fog computing the position of a fog client is known to the nodes in fog as a node is connected to the nearest fog

node. This is useful in emergency situations and also for target advertisements [4, 8].

Mobility: As fog computing provides wide geographical distribution, many mobile devices get connected to any network. The communication between devices and fog enables better mobility which is important for various fog based applications such as IoT. Fog layer provides support for both static computation resources such as banks, red light camera, etc and for mobile computation resources such as smart phones, vehicles, etc [10, 11]. Heterogeneity: Fog computing has a very heterogeneous organization structure. It provides support for the processing and collection of various types of data from different types of network capabilities. As fog nodes are present in various different environments and have diverse providers it must have the ability to interoperate them for the management of services of a wide range. Fog helps association with different places and supports various devices like 3G, 4G, WLAN, etc [3, 8].

Low latency: As fog nodes are usually very near to the device as compared to cloud, result time is cut down and the processing of data becomes faster. Due to the computing resources being present at the edge of the network, fog computing offers lowest possible latency [4, 8]. Real-time interaction: Instead of batch analysis as in cloud computing, fog computing offers real-time communications due to the presence of fog nodes and devices closer to each other. It includes gaming, streaming and augmented reality. It also helps find local network condition and traffic conditions [8, 11]. Protection and Privacy: Data security is an integral aspect in fog computing as the data generated by IoT is important and should be protected from cyber hackers. For this fog computing uses various techniques such as isolation and encryption [9, 11].

Literature review

The fog computing concept refers to the diversity of scenarios created by cloud computing environments, as well as the decentralization and localization of data-centric clouds. In comparison to cloud servers, fog devices only cover explicit information that is regularly used in it, and the volume of data in fog devices is typically much smaller. Fog only keeps data that is commonly utilized by users; the rest is received from the cloud. The goal of this area is to make data transfer across multiple domains more uniform and trouble-free. Fog computing may be assumed as a bridge between users and cloud servers, which connects users quickly and reduces the services invisibility [12].

Fog computing is a type of cloud that connects end devices and cloud. Fog computing devices can transmit a variety of fresh information. Regular inter-networking tools like set top boxes, roadside units, access points, cellular base stations, and proxy servers are commonly used in these devices. The author highlighted the architecture and properties of fog paradigm and a variety of fog computing applications and security problems [13].

In [14], author proposed new techniques so that medical records that are present in the cloud database can be secured. For accessing and storing data in a more secure manner various cryptography techniques based on pairing like a decoy

technique that uses some cryptographic algorithm. First of all, a legitimate user can access original medical databases after verifying their authenticity twice. Here we need to set a decoy medical database to confuse attacker while the original medical database is kept hidden in a cloud data-center. The data from the decoy database can be returned if the authentication failed

Many challenges in meeting security and privacy requirements are suffered by fog computing. These challenges are caused because of the issues of Fog computing resources. In time, Fog computing might also suffer from newer security and privacy issues. In [15] the author provides a detailed analysis of Fog privacy and security issues, and also identifies three groups of Fog privacy and security challenges: “network services and communications”, “information analysing”, and “end device’s privacy”.

Author put forward a model for protection of data in fog computing having the target of protecting information and also handling the mobility issue, and help find a model for data protection which enables the users to be able to access securely resource they are authorized to use based on their roles. Author presents a Region based Trust Aware model for solving the trust issue in fog nodes, a Role based Access control for access control that analyses the data protection and the performance issues. It also puts forward a management service to see the variations of users and fog devices locations [16].

In [17], author implemented user behaviour profiling (UBP) for overcoming the issues of data privacy, trust and security in mobile cloud servers that makes use of a fog computing paradigm. In the situations if an intruder tries to download the request to a valid file, then with the help of decoy techniques in Fog computing we can reduce the damage faced during insider and intruder attacks. A new policy of service broker that helps to find the right Data centre that should be allocated to a particular request of any user considering what the user requires in security response time and load are presented. Also keeping in view the changing nature of Fog paradigm, dynamic reconfiguration concept for adapting the variations in DC properties dynamically have been introduced [18].

Security issues in fog paradigm

The technique of fog has become a paramount trend oftoday as it has resolved all the technical issues and complexities that were faced in cloud computing and has set revolutionized the world of modern communication [19]. But the fact remains that even fog computing is vulnerable to various services and data related security threats. Even though fog computing has several benefits over cloud computing the security issues make the deployment of fog computing for modern systems difficult [19]. There are many critical security measures to deal with cloud related security issues. But the techniques used for safety and privacy of the existing cloud computing do not work for a fog computing network due to the properties of fog computing like heterogeneity, mobility, large-scale geo dispersion, etc. Those measures cannot be deployed in fog computing due to its diverse attributes and portability. As a result, to deal with security issues in fog computing some new mechanisms have to be deployed [20]. Various security threats of fog computing are shown in figure 3:

Fig. 3 Security threats in fog computing [20]

Trust: Trust plays a very important role in building relations among fog nodes and edge contraptions. Fog nodes are responsible for the maintenance of security and for maintaining the user's anonymity. Fog nodes have to be trusted with data and they are expected to complete the tasks with the release of only non-compromising information [20]. Thus a trust among all the fog nodes in a fog network and between fog nodes and end devices is important. The trust between fog node and end devices is ensured to maintain security. As all the fog nodes work together for managing the workload to provide real-time services, a security threat arises if anyone of these nodes is malicious as integrity is challenged. The heavy workload is processed by several fog nodes to provide services in real-time. The challenge is how integrity can be protected if one of these nodes is malicious. Fog nodes are widely distributed making them vulnerable. Any fog node or end device may coax other into interacting with them by pretending to be legitimate [21]. Trust relations between fog nodes are shown in figure 4

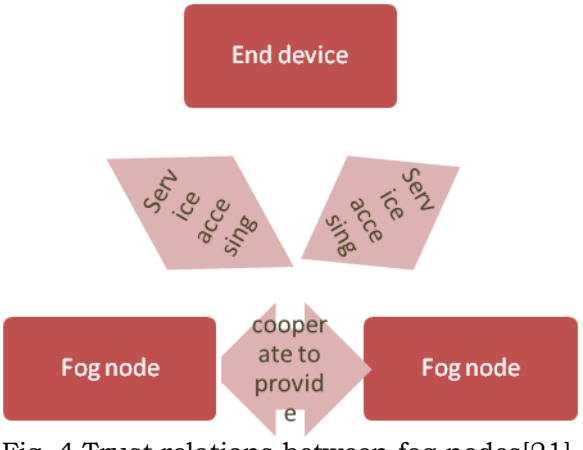

Fig. 4 Trust relations between fog nodes[21].

Authentication: One of the essential requirements among fog nodes and end devices is the feature of authentication. Authentication is said to be able to identify every node connected as a valid node. Insecure authentication is a big security issue in fog computing. There are no rigorous protocols for authentication in fog computing [22]. Mainly there are two concerns, the first is the provision of real-time services in a large area where various fog nodes track users by working together for users that are going from the spread region of one fog node to the coverage region of another. For such scenarios when the user is travelling the user has to be authenticated for each fog node before providing any services which increases the latency in provision of real- time services unnecessarily and secondly during the authentication process the identities of users should be protected from getting exposed to attackers so as to not share the current location of any user to attackers [21]. It is a very difficult task as the devices connected to the system are different in force, capacity and handling [20]. Forgery: The attacker might duplicate and copy the identity and behaviour of someone else in order to deceive a person or the security system. This is called forgery. It can reduce the performance of the network by using its resources such as storage, bandwidth and energy. Malicious users can create counterfeit data with the goal of misdirecting different substances [19, 20].

Tampering: Tampering security attack means the data that has to be transmitted might be altered by the attackers. Such kind of attacks are very hard to detect because of the reason that the users are mobile and also as the transmission medium is wireless, causing delay in the transmission of data or in some cases even failure [19]. Spam: Spam is the unwanted and unnecessary data which is produced by the malicious attackers. It includes the extra information and fake data that the attackers gather from the user. Due to spam important network resources are consumed unnecessarily. It is often misleading and used for fraud and can also cause privacy breach [19].

Jamming: Sometimes a huge chunk of information is generated by network intruders and attackers with the aim of jamming the transmission bridges and for holding the resources for a bigger chunk of time than they are entitled to which prevents legitimate users from accessing a transmission medium which is reliable and efficient. Such attack is called jamming [19]. Eavesdropping: In this type of attack, the confidential information of legitimate users is heard by intruders, without the knowledge of the user, from the transmission channel. If communication channel is compromised any unencrypted data or confidential data encrypted using inefficient encryption technique gets exposed [21]. Attack of Sybil: In sybil a fake identity is used by the attackers in order to have control on the performance and effectiveness of the fog computing structure and also to alter the dependability of the fog nodes. Untrustworthy and fake crowd sensing reports are generated by the intruders. Also they expose the private data of entitled users [19,20]. Man in the Middle: In man-in-the-middle intrusion, the intruder overhears and steals personal information of genuine users by listening between communicating nodes without the knowledge of the user who is left in dark as he does not know of the presence of attacker in between the user and the receiver [19].

Collusion: Sometimes groups of attackers collude together in order to cheat and mislead the genuine users. This attack is called collusion. A collection of fog nodes or end users are attacked by the attackers with aim to level up the effect of the intrusion [19]. Impersonation: In this type of attacks, the intruder pretends to be a legitimate server to a genuine user and making them assume they are in communication with a fog node or fig server which is genuine in order to trick them and steal confidential and personal data from genuine users without their consent and knowledge [19].

Virtual Machine Attack: In this attack any intruder hacks and attains charge of the hypervisor which creates a virtual environment in a virtual machine. Virtual machine can be attacked in four different modes: "virtual machine to virtual machine", "guest to host", "virtual machine manager outside attacks" and "virtual machine to virtual machine manager" [19]. Side-channel Attack: In this attack information about applied cryptography algorithm is gathered by reverse engineering and the attacker cracks the cryptography of the system [23].

Session Hijacking: In this attack, user session is intercepted and hijacked by an intruder with the goal of gaining access to services and the confidential data of a legitimate user [23]. Insecure API's: Application Programming Interface is responsible for controlling third party applications and for verifying a user. Many Fog providers distribute API for the use of clients. The security of API is important for the security of actual application [24].

Solutions to security challenges

These security and privacy challenges need to be solved in order to provide users a secure platform for storing, exchanging and processing of data [25]. The various solutions are: Trusted Platform Module (TRM): Fog nodes are responsible for building trust in the fog network. A consistent communication has to be created by the various fog nodes amongst themselves and between fog nodes and end devices sending data and processing requests to the fog nodes. Thus this is a very challenging task [26]. Trusted platform module or TRM helps to solve this trust issue of fog computing. The end device and the fog nodes share an extra root key. Only the data that is protected by given root key is authorized for access by the fog nodes. Fog nodes cannot access the other data. This method imposes a security measure on the data of the end devices, thus building trust between end device and fog node and also between various fog nodes [27].

Reputation-based trust model: The reputation-based trust model uses 'reputation' to build trust between various fog nodes and the end devices. Reputation is a belief about an entity based on other entities observation at a particular time and context. It provides privacy and authentication so can be used to provide trust related security in fog environment [28,29]. Trusted execution environment (TEE): TEE, as the name implies, stands for an isolated ecosystem in which integrity and confidentiality of data is maintained by ensuring that execution inside a processor is done in a secure area thus building trust in the environment [28]. Decoy Technique: The decoy security technique works for the authentication of a user's data. In this technique fake information is provided to an attacker instead of the original information. In case a security breach is caused by an attacker, the

attacker gathers the file with fake information instead of the original file that the attacker wants. This technique is termed as the decoy technique as the fake message acts like a decoy. Security is improved by creating decoy files in the start. Only the authorized users are able to access the original data [19].

PKI Based Authentication: Here authentication based on Public key infrastructure (PKI) offers transparent and easy to use certificate and services managing keys for allowing encryption and the ability of digital signatures between various nodes for helping to create a reliable networking environment which provides security to its authorized users. With the help of PKI the CIA properties: confidentiality, authentication and integrity can be ensured [28,29]. Cryptography: It refers to encrypting our data into cipher code and then transmitting it in the network. The steps followed in fog cryptography are:

a) Generation of Key
b) Encryption at client side
c) Re-encryption at fog node
d) Decryption at fog node
e) Decryption at client side

In fog environment a secret master key along with public elliptic curve parameters are used along with the fog node in key generation. The cipher text in client encryption is produced by using some random parameters along with the private key. Elliptic curve parameters are used for producing the cipher text during fog re-encryption. Then with the help of client key the intermediate cipher text is computed in decryption procedure. And at last, intermediate message is received through the private key and the actual message is found in the client side decryption procedure. This technique is the most important technique for data security [30].

Intrusion detection system: To mitigate the effect of intrusions and send alerts when an intrusion occurs, intrusion detection systems are used. The fog computer paradigm is vulnerable to various types of attacks such as Sybil, virtual machine attack, side channel attack, etc. The intrusion detection system helps detect such attacks. For this purpose, this system monitors and analyzes user registration information, a log file and the access control policy. In fog computing the system can be deployed in fog node in system side with the aim to identify illegal activities by inspecting, observing and interrogating about the access control methods, customer login information and log files with detailed questions. It might be used at the network side of fog in a similar fashion for detecting any harmful attacks such as port scanning, denial of services (DoS), etc. Thus the fog nodes benefit a lot from IDS as they monitor the VMs and the internal fog network [31]. Perimeter IDS are used in fog that help to coordinate with different IDS [19].

Biometric Authentication: This authentication technique identifies a user on the basis of various biological inputs by scanning some parts of body. It uses various features such as voice and fingerprint recognition, face recognition and iris scan. It provides high-level security but take a lot of cost to set up [28,29]. Access control: It is the method for checking if any end device or any client can use any particular part of the resources. There exist several models for access control.

a) Discretionary access control (DAC) model: In a DAC model, owner of the data decides and sets the access permissions for others. It is less secure and flexible access control method and used where convenience is required
b) Mandatory access control (MAC) model: The MAC model is the most secure and strict form of access control. It is used in multi-layer security systems where the access rights are decided by the system administrator.
c) Role-based access control (RBAC) model: It works on the principle that rather than who the subject is the role of that person in the organization is more important. In this model any user can access the data authorized for his role only.
d) Attribute-based access control model (ABAC) model: In this technique, attribute-based encryption (ABE) provides data privacy and also gives the object owner to grant access directly. The user is able to access the data if he satisfies the attribute set by the owner [10].

Blockchain Security: Though blockchain was first brought in for Bitcoin's secure crypto-currency application, but now it has been understood that they can also be utilized in cloud and fog networks pertaining to their high level security features. Some of its features are: Reduces single point failure, provides encryption algorithm with high security, ability to track status of node in an efficient manner. Blockchain technology can help in the prevention of different types of malicious offenses in fog like man-in-the- middle attack, DoS attack, etc. As it has various technologies that are very advanced for security and privacy related issues such as cryptographic hash, digital signatures and distributed consensus algorithms. They help to detect malicious activities by providing unique symmetric key pair and guide to all the devices in our network. Thus it helps to ensure security, authentication, and accuracy of information in the fog network. It can help in the detection and isolation of any malfunctioning node and isolating it from the system to avoid security breach in the whole system [28].

Virtualization: Virtualization is an important aspect in fog environment. A virtual machine monitor is set up in the middle of operating system that is the host as well as the virtual machines as guests. There is a detector that detects when an unwanted event occurs and a recorder that keeps the record of any such malicious activity, in the virtual monitor [27]. Cyclic redundancy check: Image information is protected by image compression and CRC (Cyclic Redundancy Check) [32].

Conclusions

Here, we discussed the limitations in cloud paradigm, the concept of fog computing, its architecture and different types of characteristics of fog environment. This paper also does a survey in various problems in fog computing and puts analyses the various security issues that are present in it and also puts forward various solutions for solving these security issues present in fog paradigm. Fog computing provides major improvement over cloud paradigm as it provides us several advantages like the latency issue of cloud is resolved in fog computing and latency is reduced. We have presented the methods of several techniques that can be used in solving the security issues present in fog computing. The solutions were presented on the basis of various security issues

identified in fog computing paradigm. Several cryptographic algorithms have been presented for providing security in a fog network. Various solutions for solving the security issues of trust, authentication, privacy, etc have been discussed such as TRM, TEE, access control models like MAC, DAC, RBAC, etc.

References

1. Abbasi, B. Z., & Shah, M. A. (2017). Fog Computing: Security Issues, Solutions and Robust Practices. *Research Gate*, 1–8.
2. Abdalla, P. A., & Varol, A. (2019). Advantages to Disadvantages of Cloud Computing for Small-Sized Business. *IEEE*, 1–7.
3. Ádám Mann, Z. (2020). Notions of architecture in fog computing. *Computing Springer*, 51–73.
4. Adel, A. (2020). Utilizing technologies of fog computing in educational IoT systems: privacy, security, and agility perspective. *Journal of Big Data*, *7*, 1–29.
5. Alzoubi, Y. I., Osmanaj, V. H., Jaradat, A., & Al-Ahmad, A. (2020). Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Wiley*, 1–26.
6. Arya, D. E. E. K. S. H. A., & Dave, M. A. Y. A. N. K. (N.D.). Security-Based Service Broker Policy For Fog Computing Environment. *8TH ICCCNT*, 1–6.
7. Ashi , Z., Al-Fawa'reh, M., & Al-Fayoumi, M. (2020). Fog Computing: Security Challenges and Countermeasures. *International Journal of Computer Applications* , *175*(115), 601–628.
8. Bousselham, M., Addaim, A., & Benamar, N. (2019). A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System. *IEEE*, 1–4.
9. Choudhary, A. kumar, & Rahamatkar, S. (2020). An Overview of Fog Computing: Architectures, Applications with Security Challenges. *High Technology Letters*, *26*(10), 971–992.
10. Dang, T. D., & Hoang, D. (2017). A data protection model for fog computing . *Second International Conference on Fog and Mobile Edge Computing (FMEC)*, 32–38.
11. Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. (2021). *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(6), 5081–5088.
12. H, S., & V, N. (2021). A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges. *ScienceDirect*, *7*, 162–176.
13. Iorga, M., & Goren, N. (2018). Fog Computing Conceptual Model .*NIST SP 500-325* , 1–14.
14. Kumar Singh, J., & kumar Goel, A. (2021). Study on fog computing: security & privacy challenges in terms of IoT. *Journal of Physics: Conference Series*, 1–11.
15. Lisbon, A., & Kavitha. (n.d.). A Study on Cloud and Fog Computing Security Issues and Solutions. *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, *4*(3), 17–22.
16. M J, E., Jose, J., & Jose, D. (2019). A Fog Based Security Model For Electronic Medical Records In the Cloud Database. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, *8*(7), 2552–2560.
17. M. Alwakeel, A. (2021). An Overview of Fog Computing and Edge Computing

Security and Privacy Issues. *SENSORS*, *21*, 1–20.
18. Parikh, S., Dave, D., & Patel, R. (2019). Security and Privacy Issues in Cloud, Fog and Edge Computing. *ELSEVIER*, *160*, 734–739.
19. Patwary, A. A.-N., Fu, A., & Naha, R. K. (2020). Authentication, Access Control, Privacy, Threats and Trust Management Towards Securing Fog Computing Environments: A Review. *IEEE*, *10*, 1–34.
20. Puthal, D., Mohanty, S. P., & Bhavake, S. A. (2019). Fog Computing Security Challenges and Future Directions. *IEEE Consumer Electronics Magazine*, 1–8.
21. R, R., & Kumar, R. A. (n.d.). Possible Solutions on Security and Privacy Issues in Fog Computing. *Institute of Scholars*, 234–240.
22. Rahman , G., & Wen, C. C. (2018). Fog Computing, Applications , Security and Challenges, Review. *International Journal of Engineering & Technology*, *7*(3), 1615–1621.
23. Rahman, G., & Wen, C. C. (2018). Fog Computing, Applications , Security and Challenges, Review. *International Journal of Engineering & Technology*, *7*(3), 1615–1621.
24. Rahul , S., & Aron, R. (2021). Fog Computing Architecture, Application and Resource Allocation: A Review.*Workshop on Computer Networks & Communications*, 31–42.
25. Romana, R., Lopeza, J., & Mambob, M. (2018). Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges. *Future Generation Computer Systems*, *78*, 680–698.
26. Roy, S. H. L. O. K., & JIYANI, A. N. K. I. T. A. (2018). Security and Privacy Issues of FOG Computing: A Survey. *IRE Journals*, *1*(9), 107–109.
27. Saad, M. (2018). Fog Computing and Its Role in the Internet of Things: Concept, Security and Privacy Issues . *International Journal of Computer Applications*, *180*(32), 7–9.
28. Sharma, N., & Prabha, C. (2021). Computing paradigms: An overview. *2021 Asian Conference on Innovation in Technology (ASIANCON)*, 1– 6.
29. Usha, G., Kannimuthu, S., & Karthikeyan, H. (2019). Augmentation and Orchestration of Security Techniques in Fog Computing. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(2S4), 143–148.
30. Verma, U., & Bhardwajb, D. (2018). Security Challenges for Fog Computing enabled Internet of Things from Authentication perspective. *Proceedings of International Conference on Computational Intelligence & IoT (ICCIIoT)*, 382–387.
31. Yassein, M. B., Hmeidi, I., Shatnawi , F., & Rawasheh, S. (2020). Fog Computing: Characteristics, Challenges and Issues. *International Conference on Mathematics and Computers in Science and Engineering (MACISE)*, 240–245.
32. Zhang, P., K. Liu, J., & Yu, F. R. (2018). A Survey on Access Control in Fog Computing. *IEEE Communications Magazine* , 144.