VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2023, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 11, Number 1, January-March 2023 *pp:01-11*

A Survey on Security Issues and Attacks of Fog Computing

Ramsha Qureshi[1], Muhammad Asad[2], Saima Tunio[*3], Sirajuddin Qureshi[3], Mughees Ahmed[2] and Ali Ghulam[4]

[1]Department: Department of Computer Science, COMSATS University Islamabad
[2]Department of Computer Science and Engineering, Air University Multan Campus, Pakistan
[3]Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China
[5]Information Technology Centre, Sindh Agriculture University, Tandojam, Sindh, Pakistan.
Correspondinng Email Address: saima.tunio@gmail.com

ABSTRACT
There is a link between the cloud and the Internet of Things (IoT). The layer that makes up the dispersed network environment is exactly what it is. Cloud computing is brought out to the edge of the network through the type of networking topology referred as fog computing. Users can benefit greatly from fog computing. Fog's primary role, similar to cloud computing, is to allow people mobility. Fog computing is becoming more and more popular, whereas at the same time, security dangers are growing every day. Users' identification & verification are crucial. The fact of fog computing cannot effectively utilise the security and privacy solutions provided by cloud computing must be emphasised. The risks, issues, and solutions linked to security in fog computing are outlined throughout this study. The poll then includes information on ongoing research projects as well as open security and safety concerns for fog computing.

KEYWORDS
Authentication, IOT, Fog Computing, Security, Verification

JOURNAL INFO
HISTORY: Received: January 05, 2023 Accepted: February 23, 2023 Published: February 26, 2023

INTRODUCTION

Fog computing provides many services on demand which includes online storage, platform and software services. Fog computing is very useful for all users especially for companies because they can reduce the size of their data. Fog computing is closed to edge devices. By using the Fog computing the users can virtually use the application and services provided by Fog no matter wherever they are in the world. They can also access their data stored on Fog from anywhere in the world. The cloud and indeed the end users are separated by fogs, and indeed the infrastructure is decentralised. Fog computing aims to bring data storage, computation, and networking capabilities nearby to the user while also enabling mobility for them [1].

Cisco first initiated the Fog computing and their goal to initiate the Fog computing was to enhance and extend the Cloud computing. Basic operations are typically carried out on the edge whereas distribution is done here on cloud in fog computing. Fog computing is very important for IoT devices because it provides many facilities to the users like mobility, scalability and reliability [2]. Fog computing provides mobility and a user can directly communicate with Fog and then Fog will communicate with cloud if necessary. Fog computing was introduced to provide the location awareness.

But there are many issues and vulnerabilities in Fog computing. There are many issues like access control issues. The malicious user get the access of Fog computing and they don't have fair intentions. In this paper, we'll talk about Fog computing security concerns, dangers, and attacks.

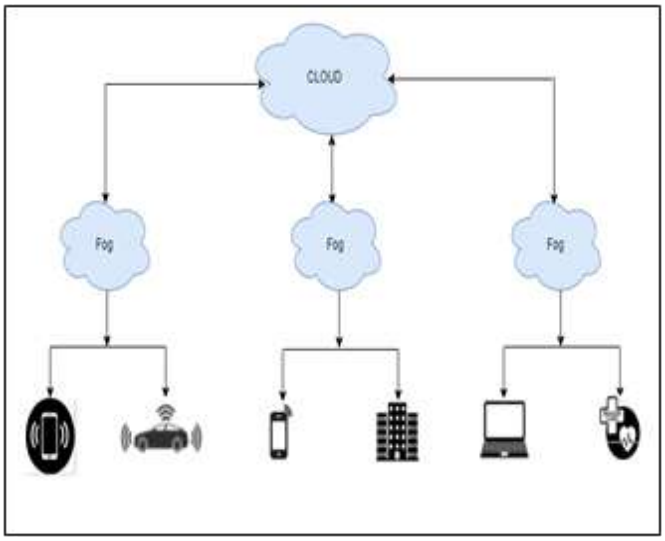

Figure 1: Cloud Computing

We will also talk about solutions to these problems.

A. 3_TIER ARCHITECTURE OF FOG COMPUTING

The most widely employed architecture for fog computing is the three tier design. The three-tier architecture is discussed below:

i) End Devices/Users:

In a fog computing system, end users as well as end devices are at the bottom level or tier. Users will interact with the fog node directly and will have immediate access to its data. These decentralised, localised nodes (of networking devices) offer information [3]. The user will communicate with the Cloud if data is not available on cloud.

ii) Fog Servers:

Fog node is the most important level/tier of Fog computing. It is crucial for computing since it is the intermediary layer that stands between both the user and the cloud in fog computing. Fog nodes, including routers, set-top boxes, proxy, base stations, and other devices, make up this system [4]. The scenario is that the fog node get the data from centralized node means cloud and then fog node directly send the received data to the end devices, additionally, it localises and decentralises the data. And the users can easily get their data through Internet communication.

iii) Cloud Servers:

Throughout the fog computing architecture, the cloud tier is the third & highest level/tier. It is a centralised data centre and just a node or server that can hold all of the data from other fog nodes or servers. The cloud node does have an enormous capacity for data storage. As a result of this significant network congestion and excessive latency, the quality of services suffers.

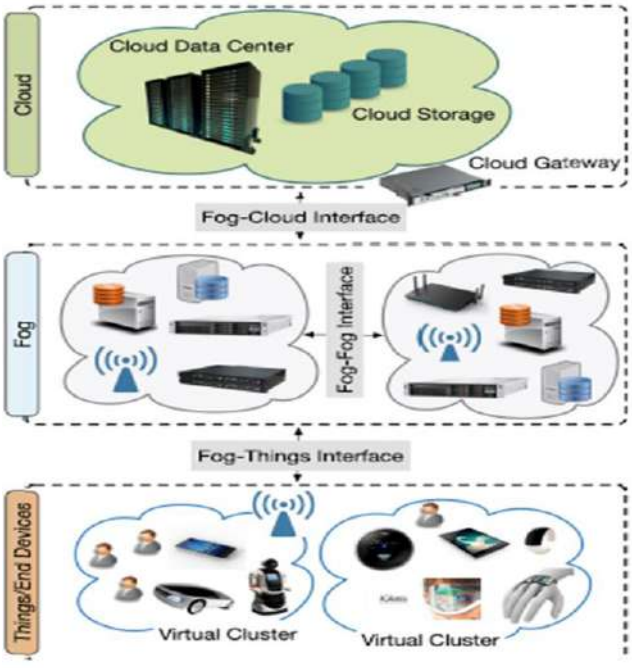

Figure 2: 3-tier Architecture of fog

iv) Fog Computing Characteristics

The following list includes some fog computing features:

1) Low Delay at the edge of the net

The usage of the IoT technology has significantly increased during the last several years. As a result, user expectations are gradually rising. Video games, for instance, have very strict criteria for delay and demand real-time system updates.

2) Widely distributed geographical location

In contrast to cloud computing, which gathers resources, fog computing is employed and is useful for geographical dispersion [5]. Fog is important because it easily fulfil the needs of our daily life.

3) Huge number of nodes

Fog computing is widely utilised because it appears to contain a significant amount of nodes [6]. There are a lot of examples of Fog computing, one of them is camera and this is used to monitor the environment around us. These cameras require very large number of nodes because it is a large scale sensor network.

4) The leading role of wireless access

In cloud computing, it is needed to process the signals of devices through the cloud but when we use fog computing, these devices can directly communicate with the Fog because Fog is directly connected to our devices [7]. As these devices don't communicate with the cloud directly the performance of the fog is very important and fog computing also provide the mobility facility [8].

5) Real-time analysis & near source control

Examining the digital cloud is essential for meaningful interaction in fog computing in order to offer services to customers.

6) Heterogeneity

Fog computing is especially helpful in daily life since it supports a wide variety of heterogeneous hardware and software devices with a range of components in a range of situations.

7) Flexibility

The facilities provided by fog computing also include flexibility, inexpensiveness and portable deployment of hardware and software.

8) Big Data Applications

Fog computing also offers the option to integrate the IoT and cloud computing for digitized big-data analysis.

9) Interoperability and federation

For certain services to be supported seamlessly, a number of suppliers must work together [9]. As a result, services must be replicated across domains and Fog components should be able to communicate with one another.

RELATED WORK

In order to illustrate the relevance of the subject that is covered in our article, in this section, we look at the studies that have been conducted primarily in the topic of fog computing and highlight the security issues that are involved.

A. **AUTHENTICATION**

According to the authors of, authentication is crucial to the protection of IoT devices. However, many IoT devices lack sufficient storage and processing power to carry out the cryptographic procedures needed for data authentication. These gadgets can do these functions using fog [10]. Yee Wei Law and colleagues presented the wide-area measurement key administration (WAKE) concept for the smart grid in. The foundation of this protocol, which uses multicast identity for secure communications, is public-key infrastructure (PKI) [11]. This concern can also be resolved with conventional PKI-based authentication.

B. MOBILE BIG DATA ANALYTICS

Regarding cloud big data architecture & mobile clouds. The analysis of big data is crucial. Fog doesn't face the high latency which occurs in cloud computing because fog provides the large scale data process system. Data is transmitted to data centres within core networks and afterwards returned to the cloud.

C. FOG COMPUTING IN IoT

The current location of cloud computing is situated at the network's edge. A typical IoT technology is fog. Fog computing is indeed the virtualization of infrastructure & components architecture that extends the cloud computing idea towards the edge of networks. Numerous securities issues arise when several devices and technologies are used together. Because fog has limited storage space and presents challenges for fog computing, many strategies cannot be implemented [12].

D. FOG COMPUTING IN MOBILE APPLICATIONS

The authors of discussed the function of fog computing across numerous portable devices. This approach's benefits, architecture, & design are all outlined. In this work, the differences between cloud computing and fog computing are also discussed. Additionally, authors discuss networking's internal computing, storage, & communication [13]. This paper also looks at scenarios and the applications related to them. The authors in describes that the end devices like mobile phones, smart objects and edge servers make the edge network. Necessary capabilities for supporting edge computation are embedded in these devices.

APPLICATIONS OF FOG COMPUTING

An increasing number of individuals are now using fog computing each day. Fog computing is frequently used. Additionally, there are numerous uses for fog computing. By the close of 2025, 45 percent of the world's data, according to a research by IDC, will be on fog and close to the edges of the network [13]. It is also stated that in the coming years, fog computing will be able to withstand AI, 5G, and IoT. According to a different IDC analysis, edge devices will contribute 10% of the world's data by 2020 [14]. As a result, it will require more effective fog computing solutions that offer reduced or minimal latency.

According to CISCO the most common applications of Fog computing are given below:

Autonomous vehicles are new technology which is being used in daily life and they are increasing day by day. Tesla is doing some work to add automatic steering and they are also enabling literal "hands free" operations of the vehicles. They are also working to add the self-parking feature in vehicles for which no person is needed behind the wheels [15]. Fog computing is very helpful for internet connected vehicles. Due to the real-time interactivity that fog computing provides [16].

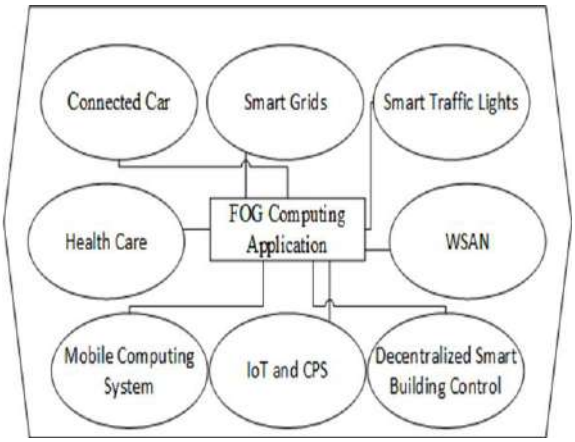

Figure 3: Applications of Fog Computing

A. CONNECTED CARS

There will be direct communication between vehicles, access points, and traffic lights. And there will come a time when connected vehicles will save lives by reducing automobile accidents. [5].

B. SMART GRIDS

A crucial use of fog computing is Smart Grid. It is founded on the need for energy, accessibility, and affordability. Other energy, like as solar and wind, can also be used by these devices [17]. Fog collects data, which is then edge-processed and used to produce control commands for actuators. Fog permits combined data storage at the top level and non-volatile memory just at bottom tier.

C. SMART TRAFFIC LIGHTS

Another possible application for fog computing is in intelligent traffic signals. After detecting the ambulance's flashing lights, it is also utilised to open lanes. Additionally, it is utilised to find cyclists and pedestrians. Wi-Fi and 5G can be used in fog computing to enhance communication between the vehicle as well as the access points [17].

D. WIRELESS SENSOR AND ACTUATOR NETWORKS (WSAN)

The original Wireless Sensor Nodes (WSNs), are also called motes. Actually they were designed to work at even at low power which extends the battery life and it also makes the energy harvesting feasible. The WSN contains low bandwidth, loss of energy, low processing capabilities, and limited memory motes that function unidirectional as a sources as well as a sink. These sensor networks' functions

include environmental sensing, straightforward data manipulation, and data transmission to the static dock. TinyOS2 is the class's contemporary standard operating system. The movements have proven useful in a variety of scenarios [18] for collecting environmental data (humidity, temperature, amount of precipitation, light intensity, etc.).

E. DECENTRALIZED SMART BUILDING CONTROL

To determine the temperature, remote sensors are integrated in the high - performance building control system, humidity or amounts of various gases in the air inside the building. Every one of the Earth's detectors may communicate information with one another in this way, and the readings can be aggregated to provide accurate measurements [19]. Haze devices engage with data through dispersed decision-making. The system is getting ready to cooperate to reduce the temperature, introduce fresh air, eliminate humidity first from air, or raise humidity. The sensors turn on or off the lights in response to movement. Smart buildings that can fulfill the fundamental requirements of indoor & outdoor energy conservation use spectacular computing.

F. IOT AND CYBER-PHYSICAL SYSTEMS

Fog computing is a crucial part of a CPS and Internet of Things. IoT refers to a network that uses the Internet & communications to link common physical items to a particular address. The CPSs feature combines the system's mathematical and physical elements. Leveraging computer-based controlling and communicating systems, systems engineering, as well as natural realities, CPSs and IoT will change the world. Fuzzy computing is built on the concept of an embedded system in which programs, programs, and computers are included [20]. Examples include connected vehicles, medical devices, etc. The objective is to combine an uncertain and dynamic environment with the idea and correctness of programs and networks. It will be able to create intelligent medical equipment, intelligent infrastructure, including robotic & agricultural technologies as computerized physical systems proliferate.

G. MOBILE COMPUTING SYSTEM

Fog creates more virtualization and computing hubs for mobile users. The Fog computing explores the changing needs of mobile phone users and often provides them with local needs [21]. Fog metres can offer all required services to mobile device users having low-latency & low-latency local contacts. As a result, smart phone customers receive higher-quality services while also spending less on bandwidth & power. Cloud computing helps bring online cloud computing and mobile computing.

H. HEALTH CARE

Health care is another application of fog computing. It is being used to facilitate the users in health care. In this field, a lot much work has taken place. A plan named FAST is proposed by Cao et al.. [16] Fog computing aided distributed analytics platform is referred to as FAST. For stroke patients, this is employed to detect falls. The inventors of this system created a fall detection algorithm that consists of time-series analysis methods, acceleration measurement algorithms, and filtering approaches that aid in the fall detection phase. They divided the jobs among edge and the cloud in their system, which operates in real-time within fog computing. Response energy consumption and time usage were comparable to methods already in use when this technology was tested.

Stantchev et al. [22] proposed the 3 design for such a modern healthcare infrastructure. With a leadership position, tiered cloud architecture, and a fog computing layer, it provides efficient architectural features for healthcare and elder care applications. This system is made more effective by the low latency, mobility assistance, location awareness, & security measures provided by the fog layer. Such a care application's process flow makes use of the Business Process Model & Notation (BPMN). After that, a service-oriented model & notation are used to map it to devices (BPMN) [23]. It was demonstrated how helpful the use case served as a model for a sensor-based, smart healthcare system.

SECURITY ISSUES AND ATTACKS

Fog computing is becoming ever more popular, which means that assaults and security concerns are also growing. There are different types of security issues and attacks which occur in fog computing. They are discussed in this section.

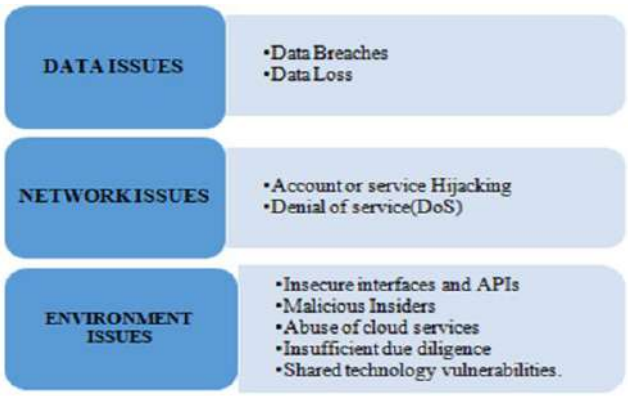

Figure 4: Security issues in fog computing

A. DATA ISSUES

Data Threats are those vulnerabilities which affects the data stored in the servers and it can exploit the information of users and servers as well [15]. Sensitive data can be breached if unauthorized users have access to the data. These malicious users can use this data for their purposes [24]. This can affect an organization and company, and this affect and loss can be huge. Some of issues of data are given below:

- Account Hijacking:

Account hijacking is another network level issue of fog computing. In this attack malicious and unauthorized

user hijack the accounts of users and try to steal the data and information of the users and use it for malicious purpose. Account hijacking is a tactic that uses phishing. The user's identity management, network monitoring, information leaks prevention technology, as well as vulnerability assessment technology can all help to solve this problem. This problem can also be avoided by using the decoy strategy [25].

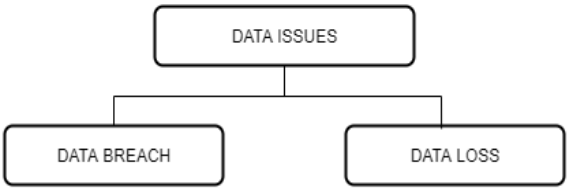

Figure 5: Data Issues of Fog Computing

- Data Breach:

Data breaching is a common issue of data issues in fog computing. In this the confidentiality of data is breached. It leads to the data leakage and this data is accessed by unauthorized and malicious users. This issue not only affects the data of users but also to the providers. The solution of the data breaching is encryption of the data [25]. Multifactor authentication is also a useful technique to overcome this issue. Decoy is another technique which can be used by fog to avoid the issue of data breaching.

- Data Loss:

Data loss is also another data issue in fog computing. Data loss is caused by data deletion, corruption of data, as well as storage errors. Cloud service provider was attacked by brute force method in 2013 and around 44 percent service providers were compromised. To prevent data loss in fog computing, it is necessary to create backups and employ data recovery techniques.

B. **NETWORK ISSUES**

In Fog computing Internet is being used to make the communication with end users more efficient. As the usage of Internet is increasing in fog computing at the same time vulnerabilities of are also increasing. Security and privacy which is needed is not being provided which are increasing the vulnerabilities on network level. Some of these issues are giving below:

- Denial of Service (DOS)

A denial of service attack (DOS) prevents authorized users from using the services offered either by fog servers. It is done by overwhelming a system's finite resources. The delay between fog services and end users occur in this attack. Intrusion detection system is used to address this attack. Another prevention from (DDOS) is to incorporate the IDS to VM. Because when IDS identifies abnormal rise of traffic, the effected application is transferred to VMs hosted on different data servers.

- Access Control Issues (ACI)

This issue cans results into poor management. And any unauthorized user can use the services provided by fog. Any user can be able to install software and change configuration

- Advance Persistent Threats (APT)

This is an online assault. The attacker's intent in carrying out this attack is to undermine the organization's security and steal its data and intellectual property [1].

- Jamming

Spreading bursts of false data over the network is how the jam communication network operates. Any kind of smart environment is susceptible to jamming.

- Eavesdropping

This attack happens when a hacker tries to understand the contents of captured transmission packets. This attack can have an impact on any fog environment.

- Man-In-The-Middle

The attacker becomes engaged in the exchange of information between two parties and has the ability to influence it. Instances of this approach in fog computing include e-Health and smart cities.

- Wormhole

In order to transfer malicious packets, the primary attacked node works with other nodes to create a path. Wormholes are the paths created by colluding nodes [26].

- Black hole

A malicious node joins the network and pretends to be a trustworthy node. Instead than forwarding the packets, it drops them. It is nicknamed a black hole for this reason.

Table 1. Data Issues of Fog Computing

Ref	Threat	Cause	Effects	Affected Security Service
[21]	Data Breach	Lack of authentication, Authorization	Malicious users can use the data for his own purpose	Integrity, Confidentiality, Availability
[22]	Data Loss	Attacker with malice, During read-write operations, there were data errors.-	Deleting data unexpectedly	Availability

Before being forwarded, black holes assault some packets [27].

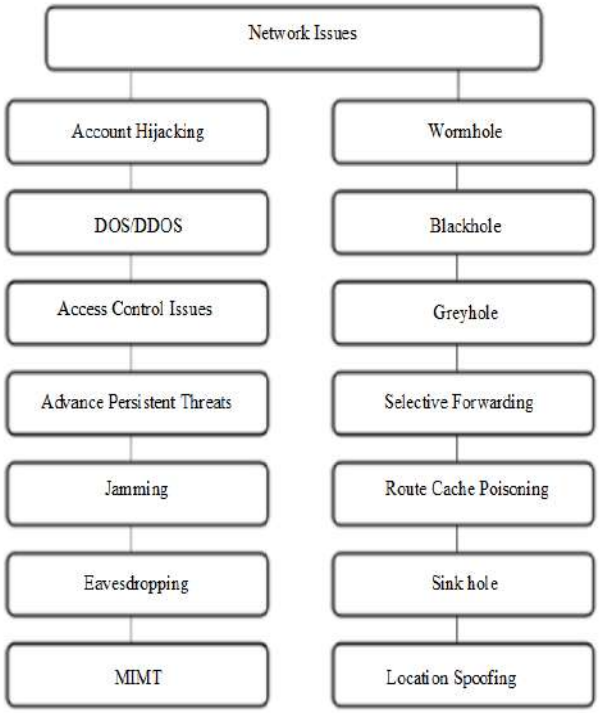

Figure 6: Network Issues of Fog computing

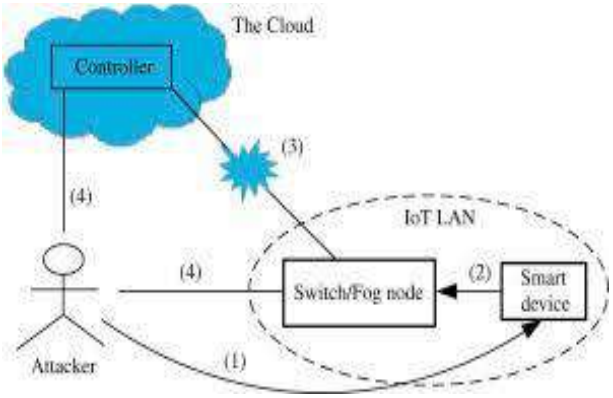

Figure 7: MITM on Fog Computing

- Grey hole

Grey hole is a new and changed version of blackhole. It tells the route that data is transmitted but instead it doesn't send the data, it is dropped by attacking node. This attack shows end-to-end connectivity that's why it is difficult to detect this attack.

- Selective forwarding

This attack results into network performance degradation because selected data packets that should be send are dropped by malicious nodes [28].

- Route cache poisoning

This attack poisons the route caches to other nodes. It is done by malicious nodes. It changes the route tables [29].

- Sink hole

Malicious nodes make it appear as though they are the best nodes to reach the target node. To accomplish it, messages are sent to the initiator node. It modifies the routing as well as other data when it receives traffic, complicating the network's topological structure as a consequence [30].

- Location spoofing

Normal network protocol operations are disrupted by this attack and malicious nodes pretend to be the nearest destined node.

ENVIRONMENT ISSUES

There are a lot of issues regarding the environment in fog computing. These issues are discussed in this section below:

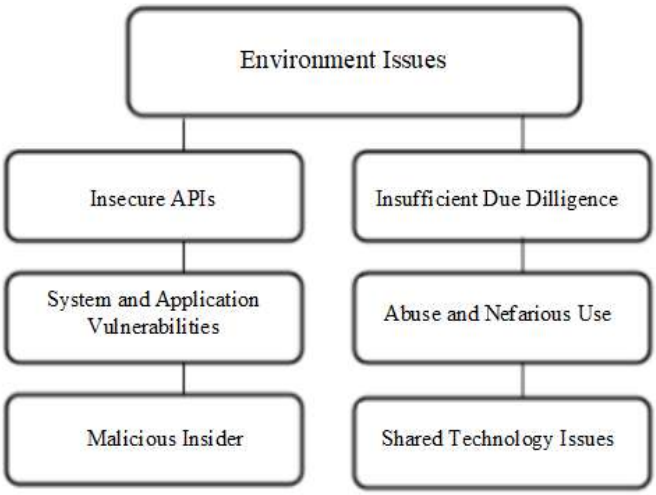

Figure 8: Environmental Issues of Fog Computing

- INSECURE APIs (IA)

There are lots of cloud/fog service providers that offer APIs (APIs). The security of just about any implemented applications depends critically on the security of APIs.

- System & Application Vulnerabilities

Software ad configuration are raised the exploitable bugs. And these bugs are used by attackers to infiltrate and compromise a system [31].

- Malicious Insider (MI)

This is an authorized user but his intentions are malicious. This user has all access to network and system of fog.

- Insufficient Due Diligence (IDD)

Any system adoption, design, as well as implementation can result in these kinds of security problems. Software-ad configuration are raised the exploitable bugs. And these bugs are used by attackers to infiltrate and compromise a system.

- Abuse and Nefarious Use

These issues occur when users get free kind of resources provided by malicious users.

- Shared Technology Issues

This threat results from sharing platforms, infrastructures, or apps. For instance, the underlying hardware may not have been intended to provide good isolation capabilities [32].

Table 2. Network Issues of Fog Computing

Ref	Attacks	Cause	Effects	Affected Security Service
[33]	Account Hijacking	Phishing, Cross site scripting, Botnets vulnerabilities	Attackers can use user's information for malicious use	Integrity, Confidentiality, Availability
[38]	DOS/DOS	Lack of authentication, authorization and internal controls	block the authorized users to access fog resources	Availability
[37]	Access Control	Lack of authentication, authorization and internal controls	Unauthorized users get access to the system	Integrity, Confidentiality, Availability
[37]	Advance Persistent	compromising the organization's infrastructure	Attacker steals the data and intellectual property	Integrity, Confidentiality, Availability
[36]	Jamming	Spreading dummy data on network	This attack jams communication network	Availability
[35]	Eves Dropping	The recording of transmission packets	Assailants attempt to decipher the content	Confidentiality
[34]	Man in the Middle	Attacker get Involved in communication of two parties	Attackers alter data that was exchanged between two parties.	Integrity, Confidentiality, Availability
[10]	Wormhole	By collusion of nodes a path is formed called wormhole	Attacker transfer the malicious packets	Confidentiality, Availability
[41]	Black hole	A malicious node is created in the path and becomes part of path	drops the packets as opposed to forwarding them	Availability
[26]	Grey hole	Black hole attack with modifications	After assaulting the node, data is lost, but it still notifies the network that information has been transferred.	Availability
[41]	Selective Forwarding	Selective data packets are dropped by attacker	Network performance degradation	Availability
[26]	Route Cache Poisoning	Route caches are poisoned by malicious node	Alteration of route tables occurs	Availability
[41]	Sink hole	Malicious nodes pose as the best routes by providing the initiator node bogus signals.	Route as well as other data are altered, which complicates the network's topological information.	Availability

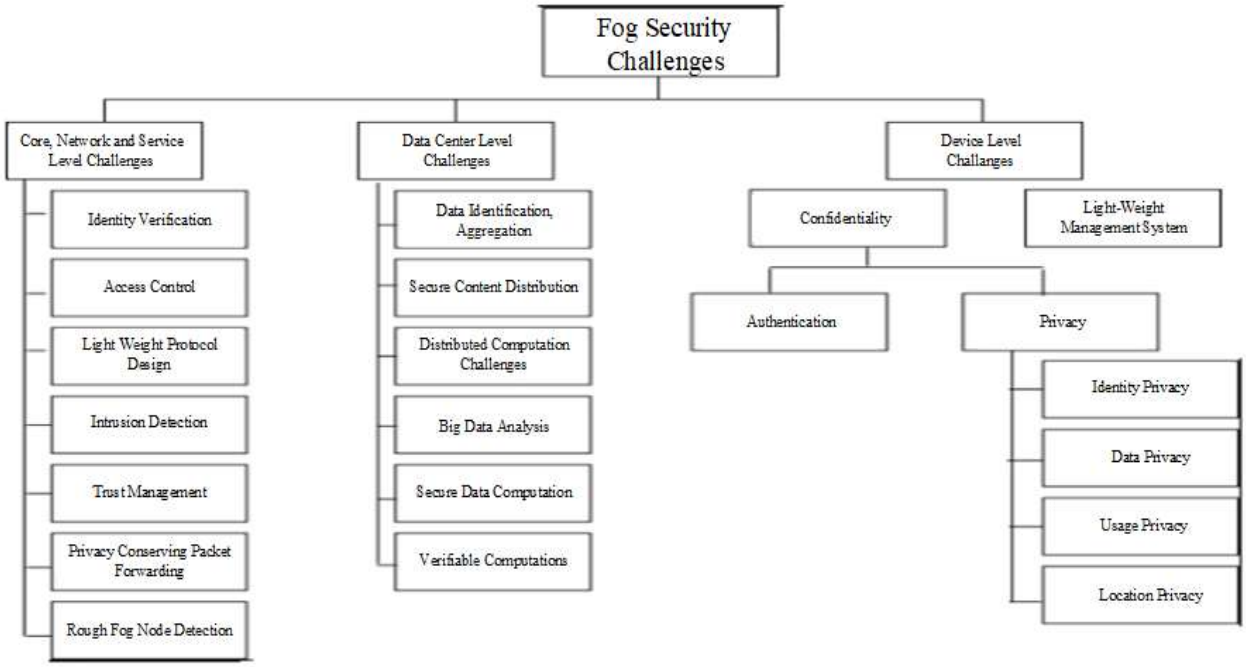

Figure 9: Countermeasures of Security Issues in Fog Computing

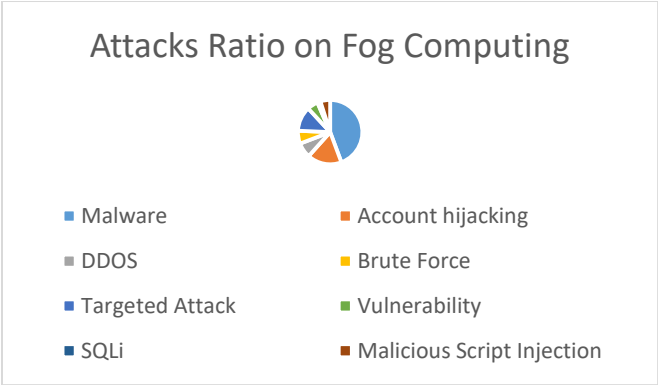

Figure 10: Attack Ratio on Fog Computing

Table 3. Countermeasures of Security Issues of Fog Computing

Challenges	**Solutions**	**Limitations**	**Security Level**
Identity Verification	Identity authentication, Co- operative authentication,	Difficult to manage the increased number of users Redundant authentication efforts are needed Cooperation of fog nodes is needed Privacy preservation is needed	Core-network and service level
Access Control	Role-based Access Control policy, Attribute-based Access Control policy, Device and key management	Strong credential handling policies are Core-network and needed to ensure trustworthiness Multiple device management is needed when access by single user Key management is needed	Core-network and service level
Lightweight Protocol design	Lightweight cryptographic techniques	Need to design efficient lightweight protocols to support real time	Core-network and service level

	Lightweight elliptic curve cryptosystem	services of fog assisted IoT applications service level	
Intrusion Detection	Host-based Intrusion Detection system (IDS),Network-based IDS, Distributed IDS	It is challenging to design a robust, Core-network and reliable and efficient IDS Local as well as global intrusion detection systems are needed in fog computing	Core-network and service level
Data identification, aggregation and integrity	Symmetric and Asymmetric encryption, Homomorphic encryption	Overhead of identifying sensitive data Data integrity verification Is Security comparatively less efficient Difficult to protect sensitive data due to the large	Data Center Level Security
Confidentiality	Authentication protocols, Privacy preservation	Scalability issues Device Level High computation cost Key management is needed.	Data Center Level Security
Lightweight-Trust Management	Trust-based routing protocols	Trade-off between computation cost and Device Level Security specific Compatibility issues with resource-Security constrained IoT devices	Data Center Level Security

OPEN ISSUES AND CHALLENGES

The majority of cloud computing is cloud secured. Due to a number of factors, not all security mechanisms can simply be applied to fog computing. The challenges of open search in terms of privacy and security are covered in this section [39].

A. TRUST

Trust is the main issue of fog computing. There should be trust in the structure of fog computing. Otherwise it will not be a secure system. There is still a lot of work which should be done in the field of fog computing.

B. PRIVACY PRESERVATION

The resources of the bodies of the EU are also shared among other things geographically close devices for support vehicles, location, mass data and more. EU information needs protection in a very secure environment Net enrollment rate [40]. As a scenario of use, in, in which the drone Integrated IoT platform based on air vehicles (UAV) for. It is proposed to integrate drones into cyber fog, Attackers through communication attacks like Mid-Man Attack (MITM) can easily take advantage of this platform for the disclosure of sensitive information such as website e Identity fog contract [41].

C. AUTHENTICATION AND KEY FRAGMENT

Among the most crucial security concerns with fog computing is authentication. Fog computing uses multi step verification to identify users at several levels of authentication F-RANS is a technique which is used in dynamic traffic and it should be addressed in future work.

D. INTRUSION DETECTION SYSTEMS

Intrusion detection systems are utilized in fog computing to recognize & thwart a variety of threats, including scan assaults, DoS attacks, Man-In-The-Middle threats, and much more. They can be used in smart grid etc. IDS should be applied on all levels of fog computing. If we secure one level of fog and don't consider others then this will not be enough.

CONCLUSIONS

Fog computing will expand the possibilities of the clouds by increasing its efficiency and effectiveness and providing mobile users with access to content & apps by utilizing their location - based services [42]. However, because of its functions and improved characteristics, fog computing raises a lot of security concerns. We overview these threats in this paper and gave some solutions. In fog computing, there remains a big demand for security and confidentiality measures.

CREDIT AUTHOR STATEMENT

Ramsha Qureshi: Conceptualization, Methodology, Software **Muhammad Asad.**: Data curation, Writing- Original draft preparation. **Saima Tunio**: Visualization, Investigation. **Sirajuddin Qureshi**: Supervision.**: Mughees Ahmed**: Software, Validation.: **Ali Ghulam:** Writing- Reviewing and Editing.

COMPLIANCE WITH ETHICAL STANDARDS

It is declare that all authors don't have any conflict of interest. Furthermore, informed consent was obtained from all individual participants included in the study.

REFERENCES

[1] T. H. Luan, L. Gao, Z. Li, Y. Xiang, G. Wei, and L. Sun, "Fog computing: Focusing on mobile users at the edge," *arXiv preprint arXiv:1502.01815*, 2015.

[2] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991–3005, 2016.

[3] D. Beli, "'. National Identification and Authentication System." 2015.

[4] L. Yang, J. Cao, Y. Yuan, T. Li, A. Han, and A. Chan, "A framework for partitioning and execution of data stream applications in mobile cloud computing," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, no. 4, pp. 23–32, 2013.

[5] Y. Gu, J. Chanussot, X. Jia, and J. A. Benediktsson, "Multiple kernel learning for hyperspectral image classification: A review," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 55, no. 11, pp. 6547–6565, 2017.

[6] S. Zhang, C. Zhu, J. K. Sin, and P. K. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Letters*, vol. 20, no. 11, pp. 569–571, 1999.

[7] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A survey of security in cloud, edge, and fog computing," *Sensors*, vol. 22, no. 3, p. 927, 2022.

[8] A. Archana Lisbon and R. Kavitha, "A study on cloud and fog computing security issues and solutions," *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, no. 03, pp. 17–22, 2017.

[9] R. Huang, Y. Sun, C. Huang, G. Zhao, and Y. Ma, "A survey on fog computing," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2019 International Workshops, Atlanta, GA, USA, July 14–17, 2019, Proceedings 12*, 2019, pp. 160–169.

[10] S. P. Brady *et al.*, "Understanding maladaptation by uniting ecological and evolutionary perspectives," *The American Naturalist*, vol. 194, no. 4, pp. 495–515, 2019.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *2010 Proceedings IEEE INFOCOM*, 2010, pp. 1–9.

[12] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *arXiv preprint arXiv:1609.01107*, 2016.

[13] A. Rani and B. Raman, "An image copyright protection scheme by encrypting secret data with the host image," *Multimedia Tools and Applications*, vol. 75, pp. 1027–1042, 2016.

[14] J. Yakubu, S. M. Abdulhamid, H. A. Christopher, H. Chiroma, and M. Abdullahi, "Security challenges in fog-computing environment: a systematic appraisal of current developments," *Journal of Reliable Intelligent Environments*, vol. 5, pp. 209–233, 2019.

[15] S. Sridhar, R. Sathishkumar, and G. F. Sudha, "Adaptive halftoned visual cryptography with improved quality and security," *Multimedia Tools and Applications*, vol. 76, pp. 815–834, 2017.

[16] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 414–454, 2013.

[17] S. Kunal, A. Saha, and R. Amin, "An overview of cloud-fog computing: Architectures, applications with security challenges," *Security and Privacy*, vol. 2, no. 4, p. e72, 2019.

[18] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," *Computer Networks*, vol. 101, pp. 192–202, 2016.

[19] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE transactions on parallel and distributed systems*, vol. 25, no. 2, pp. 384–394, 2013.

[20] Y.-W. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, and A. M. Barmawi, "Exploiting the error correction mechanism in QR codes for secret sharing," in *Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I 21*, 2016, pp. 409–425.

[21] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 2012, pp. 13–16.

[22] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[23] F. Buccafurri, G. Lax, and A. Russo, "Exploiting digital identity for mobility in fog computing," in *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*, 2019, pp. 155–160.

[24] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[25] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, no. 1, pp. 1–22, 2017.

[26] S. Roschke, F. Cheng, and C. Meinel, "Intrusion detection in the cloud," in *2009 eighth IEEE international conference on dependable, autonomic and secure computing*, 2009, pp. 729–734.

[27] S. Anwar *et al.*, "From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, p. 39, 2017.

[28] A. Lee, "Guidelines for smart grid cyber security," 2010.

[29] M. H. Ibrahim, "OCTOPUS: An edge-fog mutual authentication scheme.," *Int. J. Netw. Secur.*, vol. 18, no. 6, pp. 1089–1101, 2016.

[30] A. R. Vinod, B. S. Sunidatta, K. U. Rani, and P. P. Sasidharan, "Hindering data theft attacks through fog computing," *International Journal of Research in Engineering and Technology*, vol. 3, no. 09, pp. 427–429, 2014.

[31] C. Dsouza, G.-J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in *Proceedings of the 2014 IEEE 15th international conference on information reuse and integration (IEEE IRI 2014)*, 2014, pp. 16–23.

[32] R. Charanya, M. Aramudhan, K. Mohan, and S. Nithya, "Levels of security issues in cloud computing,"

International Journal of Engineering and Technology, vol. 5, no. 2, pp. 1912–1920, 2013.

[33] Y. W. Law, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 34–41, 2013.

[34] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128–134, 2017.

[35] G. D. Abowd, A. K. Dey, P. J. Brown, N. Davies, M. Smith, and P. Steggles, "Towards a better understanding of context and context-awareness," in *Handheld and Ubiquitous Computing: First International Symposium, HUC'99 Karlsruhe, Germany, September 27–29, 1999 Proceedings 1*, 1999, pp. 304–307.

[36] X. Huang, R. Yu, J. Kang, N. Wang, S. Maharjan, and Y. Zhang, "Software defined networking with pseudonym systems for secure vehicular clouds," *IEEE Access*, vol. 4, pp. 3522–3534, 2016.

[37] S. Smalley and R. Craig, "Security enhanced (se) android: bringing flexible mac to android.," in *Ndss*, 2013, vol. 310, pp. 20–38.

[38] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1143–1155, 2017.

[39] A. Manzoor, A. Wahid, M. A. Shah, A. Akhunzada, and F. F. Qureshi, "Secure login using multi-tier authentication schemes in fog computing," *EAI Endorsed Transactions on Internet of Things*, vol. 3, no. 11, 2017.

[40] A. Lysyanskaya, R. Rivest, and A. Sahai, "Pseudonym Systems. Selected Areas in Cryptography: 6th Annual International Workshop, SAC'99, Volume 1758 of Lecture Notes in Computer Science." *Springer-Verlag*, 1999.

[41] M. Khodaei, H. Noroozi, and P. Papadimitratos, "Scaling pseudonymous authentication for large mobile systems," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 174–184.

[42] P. Viola and M. J. Jones, "Robust real-time face detection," *International journal of computer vision*, vol. 57, pp. 137–154, 2004.