*International Journal of Engineering & Technology*, 7 (2.7) (2018) 335-340

**International Journal of Engineering & Technology**

*Website: www.sciencepubco.com/index.php/IJET*

***Research Paper***

# A survey on fog computing: research challenges in security and privacy issues

**T.Veerraju[1]*, Dr. K. Kiran Kumar[2]**

*[1] Research scholar, Dept. of CSE, K L E F, Green Fields, Vaddeswaram*
*[2] Professor, Dept. of ECSE , K L E F, Green Fields, Vaddeswaram*
**Corresponding author E-mail: veerarajut108@gmail.com*

## Abstract

With the rapid advancement of Internet of Things has enabled to combine the intercommunication and interconnection between seamless networks. Cloud computing provides backend solutions and one among the most prominent technologies for the users, still cannot be solved all the problems such as latency of real time applications. However, a new computing paradigm comes in to the picture. Many of the researchers focused on this exemplar known as Fog/Edge computing, which has been planned to the extension of cloud services. Fog provides the services to the edge of the networks, which makes communication, computation and storage for end users through fog devices and for servers like controllers. We analyze the study, which aims to augment low bandwidth, latency along with the privacy and security. The major problem in the Fog computing is security due to the limited resources. In this paper, we investigated the protection issues and confrontation of Fog and also provide countermeasures on security for different attacks. We focused the future security directions and challenges to address in fog networks.

***Keywords***: *Attacks; Cloud computing; Fog computing; Internet of things; Security and Privacy.*

## 1. Introduction

In the present scenario of the user needs are relying and considerable to increase in the no. of IoT devices/nodes to a large extent. Internet of Things allows RFID, sensor nodes and GPS in our daily life environment to active participants by getting and sharing information with other members of the network. In 1999, the IoT concept was introduced at MIT. In an Information Space, We are able to connect different objects that includes people, machines, and things anywhere at any time with the development in the areas such as Internet of Things (IoT), Cyber-Physical System (CPS) and Mobile Internet[1]. To assist with the computational and storage requirements of real time applications of distributed environment a new computing paradigm have been introduced named “Fog Computing”. Fog computing is residing in IoT environment and placed very closer to the users and IoT devices on the edge of the network. Fog computing is extends Cloud based computing in terms of storage and networking facility and reduce the latency in order to address bottlenecks in IoT applications in cloud computing. In 2012, the CISCO was introduced the theory of Fog computing.

In era of Fog, every object and devices are not only interconnected but also interacted with each other, which making it possible to recognize events and changes in their surroundings. The benefits of IoT are unlimited and its implementations are altering based on the way we live and work by saving the time and resources and offering many more possibilities for growth, innovation, and the transfer of information among different entities. By 2020, it is envisage that Internet of Things will significantly expanded by crossing 50 billion outstandingly specialized devices (that excludes PCs, tablets and smart phones), which is an remarkably large number. As a result, the extinction of the interconnected entities of an outsized network will definitely cause new security, privacy and trust threats that situate all those devices at a high risk, thus harming the affiliated users [2].

To remediate the above issues, Fog computing is advised to use the resources of computing at the close propinquity to users that helps to achieve process locally, store thereby sinking the amount of transmission needed on network and corresponding latency. Computation in Fog, which flawlessly amalgamates network edge devices with cloud centre, is showcased as an extra successful elucidation to allow and deal with said limitations. Computing architecture of Fog is distributed geographically, in which various devices of type heterogeneous are ubiquitously connected at the edge of network that can provide a collaborative elastic computation, communication and storage services [3].

Fog computing is the only new paradigm which addresses the security threats in the rapid development and ampler adoption of IoT devices in our lives. In view of the fact that the devices which are interconnected have a straight through impact on user lives and in an urgent need for a well-defined classification of security vulnerabilities and a proper security infrastructure. The new systems and corresponding protocols which can alleviate the security confront in Fog. We define the security most well-known attacks on Fog systems. It introduces the category of the attacks based on the layers in the IoT [4]. We focused mainly attacks on the various layers of the IoT architecture. It suggests future security directions to cover the diversity of challenges in IoT-Fog based networks.

The remaining part of the paper is planned as follows. Sec.2, discussed, an overview of Fog computing. After that, in Sect. 3 the related work done on Fog system. We describe the characteristics and challenges of security in Fog system in Sects 4 and Sect 5 respectively. Then Sect. 6 establishes new security directions to countermeasure these threats and finally Sect. 7 concludes the paper.

## 2. An overview of Fog computing

A Fog computing environment is very similar to the traditional networking, which is also composed with various components such as switches, routers, set top boxed, Base Stations (BS) and proxy servers, etc. and is positioned at closest propinquity of IoT devices/sensors at the edge of the network as shown in Fig. 1. The above components can support IoT applications, which are issued with diverse computing, storage, networking, and etc. capabilities [5]. The cloud-based services are centralized, Fog computing enables the network components to create a large geographical distribution. Moreover, Fog computing facilitates low latency and location awareness, end device mobility, support geographical distribution, wireless access, heterogeneity, interactions of real-time, scalability and interoperability. Thus, Fog computing can attain efficiency in terms of service latency, utilization of power, traffic on network, expenses related to capital and operational, distribution of content, etc. Thereby, Fog computing enhanced the IoT application requirements used cloud services [6]. Nonetheless, the Fog computing concept is exceptionally a lot comparable to the accessible computing paradigms.

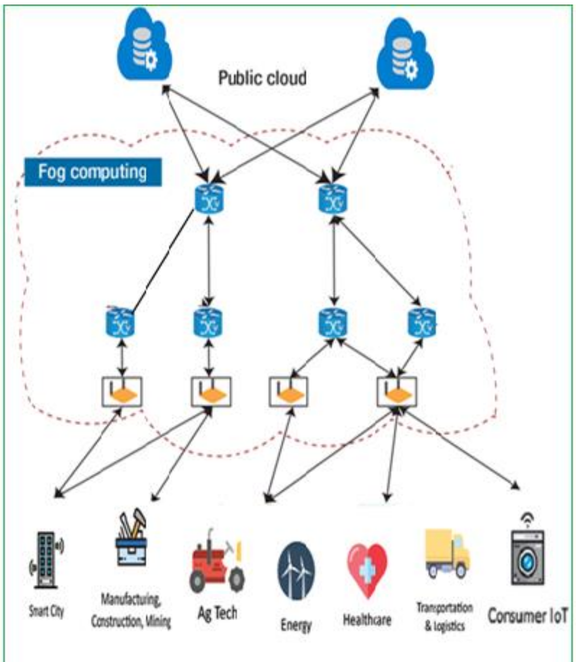

Fig.1: Fog Computing Environment

Fog computing is expandable to the networks of wireless like Mobile Edge computing and cloud computing of Mobile enables edge network computation. Fig.2 had shown the various computing paradigms. As a result, multi-tire functional operation and overhaul demand alleviation of huge number of IoT devices/sensors can easily be observed through Fog computing. Fog computing can extend cloud based services like IaaS, PaaS, SaaS, etc. to the edge of the network as well [7]. Based on the features mentioned above, Fog computing is measured as more appropriate and well-structured for IoT when compared to the other related computing paradigms.

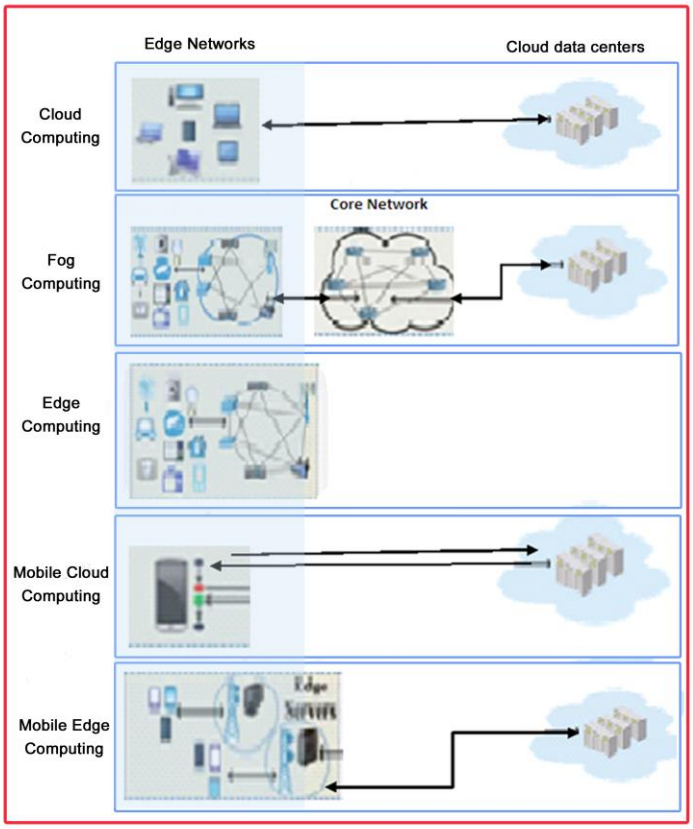

Fig.2: Computation domain of various computing paradigms

## 3. Related Work

With the study of the Cloud computing, a new computing paradigm has entered to provide various computation services to the users across the internet. However, the extent of clouds are physically centralized which are far-a-way from the proximity to end users. Due to this as a result, the clouds often endures latency, holdup in round trip, clogging in network and decrease quality etc., To resolve these issues a new paradigm comes to the picture named Fog Computing. We have been studied security challenges and mechanisms in cloud security. The security mechanisms in cloud are not sufficient and suitable for Fog environment. Security in Fog research has not comprehensively investigated how to provide a proper classification of security challenges. However, most of the research papers address only specific types of threats based on specific security objectives [8] [9]. Most of the authors address various attacks like man in the middle attack, sinkhole attack, node capture attack etc. Compared to the previous work after investigation of many papers, our paper focuses to provide a more extensive list of attacks and countermeasures.

Redowan Mahmud et al [10] Presented Fog computing taxonomy in relation to the identified security challenges and its important features. They also reviewed various computing paradigms such as Mobile Edge Computing (MEC), Mobile Cloud Computing (MCC) and Edge computing which extensions of Cloud are computing. They also presented various security aspects and their challenges.

Khan et. al [11] Presented a draft copy on applications of Fog computing to enable us to identify the common security problems. The ample collection of functionalities obsessed applications increases various security issues like data, network virtualization, malware and monitoring. It is also determined on the impact of the security issues and the possible solutions, future directions to implement the various solutions for Fog system.

Jatinder Singh et al [12] focused on security deliberation on IoT environment from the outlook of cloud users. They also discussed various managements such as resource management, data management, Identity management and trust management. It is identified and described security related considerations like issue of malicious things; issue of certifications, issues of trust associated with the large scale of IoT and decentralized Fog services.

Shanhe Yi et al [13] presented different characteristics and features of Fog computing, and discussed security and privacy issues such as storage of data, security computation and security of network. They also highlighted the privacy relevant to location, data and user which may face challenges and changes.

Jie Lin and Wei Yu et al [14] explored relationship between CPS and IoT and are presented to enhance the existing architectures, enabling the technologies, issues of privacy, security and the amalgamation of IoT and Fog computing and their applications. It also discussed several applications in fog based IoT environments that also includes the smart grid, smart transportation and smart cities are to be operate in real world environment.

Mithun Mukherjee et al [15] describe an overview of existing security and privacy concerns, their survey highlighted ongoing research efforts, open challenges and research trends security and privacy issues for Fog computing.

# 4. Security characteristics of Fog Network

There is a need to identify the characteristics of security in Fog environment which is a new paradigm. Considering the Fog network in IoT is the middle layer which is integrated edge devices and network infrastructures like Wireless sensor networks, RFIDs based sensor networks, Cloud Computing, IoT, the Internet etc. Fog environment has heterogeneous nodes and networks, all of the security challenges and threats possible to arise from the coexistence and association of the various technologies. The most enviable security objective of Fog is to protect the collected data, because the data collected through physical devices may also include sensitive user information. The Fog system required to be flexible regarding data-related attacks and offers trustworthy, data security and privacy. We study various characteristics and goals in different levels in Fog Infrastructure.

## 4.1 Secure Communication

The unauthorized access of information needs to be prevented by the secure communication. The sensitive data might be transmitted between the nodes. A secure channel establishes to defend communication from both eavesdropping and interference. There are some services to motivate the secure communication.

- *Confidentiality*: Confidentiality can ensure to prevent eavesdropping and data leakage, also ensure that the data is accessible to only authenticated users right through the process. In Fog network, a large number of nodes can be integrated. The data collected devices will not reveal the securing information with their neighboring devices. In order to provide highest levels of confidentiality, enhance techniques including Public key Infrastructure model and certificate authority.

- *Integrity*: The transmitted data in communication networks cannot be tampered or modified then protecting data from interferences. The data integration is most important feature for Fog applications. The objective of Fog to avoid forged or tempered data may give the wrong feedback. Secure data integrity mechanisms should be developed to achieve acceptable data integrity.

- *Availability*: Services cannot be scheduled which are available at all times for authorized users When ever, the data and devices are requested. One the most serious threats in Fog network are availability of the node. We study and application of techniques is very much needed to ensure availability in Fog.

## 4.2 Access Control for Fog

It controls the access of unauthorized devices to regulate the Fog recourses. Access control makes sure that the correct nodes access the appropriate data and services. In Fog environment, a challenge for access controls that interacts between the dynamic devices. There are two aspects to control the access. These are *authentication* and *authorization*.

- Authentication can ensure that no unauthorized nodes can connect to Fog network. On the other hand, data can deliver to the legitimate devices and networks. Fog contains a dynamic environment with the large number of diverse objects. However, it is very difficult to design an efficient authentication process to treat with the verification of nodes or things in Fog.
- Authorization follows the authentication, as once the node is identified. It takes care about their rights and privileges. Authorization policy ensures authenticate the node and provide privileges, which might allow them to access the services.

## 4.3 Trustworthiness of Fog

Deals with the how much trust concern can be placed in Fog network. It trusts during the interactions among and across dissimilar objects in heterogeneity networks in Fog layer. Security and privacy can be enforced with the help of trust. Modern advancements in hardware technologies enable new levels of trust, providing Trusted Platform Modules (TPM). Efficient trust management systems needed to raise the level of trust to implement trust objectives in Fog.

## 4.4 Data Sharing in Fog

Each node is uploaded the data to the Fog server and isolated from other nodes. Fog ensures the data can be uploaded to the cloud. The policy driven enforces processing the data from multiple streams. Therefore, have a requirement for both protection and sharing according to the policy. One approach of data sharing being investigated is *Information flow Control* (IFC) where data sharing policy is defined to administer the nodes in Fog system.

# 5. Security and Privacy challenges of Fog

Security challenges are predominant in fog computing. In this section, we presented the detailed security challenges in Fog Network. Fog computing considers the architecture of SOA. The network layer is established between the service layer and application layer. Hence, Fog computing is designed ahead of traditional networking components, which are highly vulnerable security attacks. The enlargement of security measures in Fog systems are rapidly moving ahead and the existing publications do not contain adequate detail evaluation. We provide a summary of security attacks in Table 1 with respect to each level in Fog systems.

## 5.1 Node level attacks

These kinds of attacks are physical attacks, which are focused on the edges of network which are very near to the users in the Fog system. The attacker needs to be physically close to the network and attempt to forging collected data and destroying the perception nodes like sensors, actuators, RFIDs, etc.

*1) Node capture attacks:* The adversary initialize physical attacks on node which is damaged, remove or compromise. Sometimes, it is possible to the adversary by physically changing the entire node or some part of its hardware can be scratched or even electronically passing the messages to extract security information from the nodes and alter sensitive information to a sensor node. These kinds of attacks can have serious connotations on the Fog network. Monitoring sensor nodes to detect and provide cryptographic algorithms against the node capture attack.

*2) Node Jamming:* This is also Denial of service with the difference that these kinds of attack are based on the Wireless Sensor networks. The adversary can obstruct with the malicious nodes of the wireless sensor nodes, blocking the signals and refused the communication. The attacker intentionally interferes to block the legitimate communication and deny the service of the Fog network. Fog also needs to define to address the Jamming problem, countermeasure mechanisms.

*3) Malicious code injection on node:* The attacker injects malicious code on the node to gain the control of the Fog system. The attacker able to execute the malevolent code meant to hoax the application into accessing to the protected information. Code authentication mechanisms need against the malicious code injection in Fog systems.

*4) RF Interferences and Eavesdropping:* The adversary can create and send noise signals over the Radio Frequency signal. The noisy signals are interfere to communicate by RFID signals. Therefore, effective noise filtering methods need to avoid the interferences of the signals. The Communication in Fog network is mostly wireless links which can be eavesdropped by unauthorized users. Hence, secure cryptographic encryption algorithms and key management schemes needed against eavesdropping.

*5) False data injection attacks:* Nodes or devices are captured by the adversary to send the false data or information to other nodes in Fog system. False data being received by the nodes, they deliver erroneous services, impacting the efficiency of Fog applications and network.

*6) Replay Attacks*: the adversary can be transmitted data to the destination node by using malicious node or device with justifiable information of identification which has been attained by the target node, in a quest to make the malicious node or device to gain the trust of Fog network. Replay attacks are commonly introduced in the process of authentication to destroy the identification validity. In Fog network, more schemes (secure time stamp schemes, etc.) should be designed and developed to mitigate the replay attack.

*7) Cryptanalysis attacks:* A cryptanalysis is applied to obtain the internal mode of operations and the encryption key which was used in encryption algorithm. However, the efficiency of the algorithm is high then cryptanalysis attack is low. But, new attacks with more efficiency, to name the attacks of side channel, can be well introduced by the adversary. Algorithms of Efficient and Secured encryption, key management schemes are required to be designed and developed in Fog to mitigate the side channel attack.

*8) Sleep deprivation attacks:* Due to the low power ability of the most devices in Fog and to enlarge the life cycle of devices or nodes, they are programmed to follow a sleep routine to enable the reduction of the power consumption. Wherein, the attack known as sleep deprivation can possibly break the programmed routines of sleep and remain the devices or nodes awake for the total time until they are completely shut down. One possible solution to extend life cycle of the devices and nodes is by using energy harvest scheme. In-addition to that, the other techniques such as secured duty-cycle mechanism need to be studied to mitigate the attack of sleep deprivation in Fog.

## 5.2 Network Attacks

These kinds of attacks are focus on communication across the Fog network which lies to conventional network. In Fog network, most of the devices are connected via wireless communication links. The network resources highly impacted by the security attacks in the distributed environment like data storage, data sharing and data searching.

*1. Denial of service (DOS):* DOS attacks can bring down the rendering services of Fog network by aiming to attack protocols of network or by shelling the Fog network with high traffic. DOS attack is known to be the most commonly used attack which signifies a category of attack that could result in Fog systems services being unavailable. In consequence, the attacks of DOS can be initiated by attack schemes, also includes Ping of Death, Teardrop, UDP flood, SYN flood, Land Attack, etc.

*2. Spoofing attacks*: Spoofing attacks are mainly used by the attacker to obtain complete access to the Fog network and sent forged data into the network system. In Fog, some examples for the spoofing attack are IP spoofing and RFID spoofing, etc. In the attacks of IP Spoofing in Fog system, the attacker may impersonate and record the valid IP address of other formal devices and then access Fog network in order to launch against fog devices steel the data and send malware data with attained valid IP address, thereby making malicious data appear to be legitimate. In RFID spoofing attack, the attacker with the ability to spoof and record the information of a valid RFID tag. Thereafter by using the valid tag ID, the adversary can send malware data to the Fog system. Possible solutions such as secure trust management, identification and authentication are used to shield against the attacks of spoofing.

**Table 1**: Classification of Attacks

| **Levels of Attacks in Fog** | **Types of Attacks for the specific levels** | **Countermeasures for all levels in Fog** |
|---|---|---|
| Node level Attacks | • Node capture attacks<br>• Node jamming<br>• Malicious code injection on node<br>• Physical damage of the node<br>• RF interferences and Eavesdropping<br>• False data injection attacks<br>• Replay attacks<br>• Crypt analysis attacks<br>• Sleep deprivation attacks | • Device Authentication<br>• Data Confidentiality<br>• Data Integrity<br>• Secure booting by using low power Cryptographic hash functions<br>• Data Anonymity<br>• Access Control Devices<br>• Physical barriers<br>• Monitoring devices |
| Network level Attacks | • Denial of Services (DoS)<br>• Spoofing attacks<br>• Sink hole attacks<br>• Man in the Middle attacks<br>• Routing information attacks<br>• Sybil attacks<br>• Unauthorized access<br>• RFID cloning<br>• Traffic analysis attacks | • Network Authentication mechanisms<br>• Confidentiality and Integrity of transmitted data<br>• Implementation of routing security<br>• Secure user data on devices by using encryption and cryptographic mechanisms |
| Application level Attacks | • Phishing attacks<br>• Malicious Virus/Worms<br>• Trojan horse<br>• Ransom ware<br>• spyware | • Access control lists<br>• Firewalls<br>• Protective software's<br>• Intrusion detection mechanisms<br>• Trust management |

*3. Sinkhole attacks*: The mainly focused in Fog networks to gather the information from the nodes of many to one communication approach, when an intruder attracts nearby nodes with false routing information. These types of attack is basis of an important threat to Fog networks and breaches the secrecy of the information and also deny the service to the network by dipping all the packets of low power, computation and communication instead of sending them to the required destination. To be cautious, sinkhole attack has the ability of not only breaking the confidentiality of the delivered data; it also acts as an essential move to launch more attacks (DOS attacks, etc.). To guard against the sinkhole attack, enhanced techniques like secure multiple routing protocols need to be further studied and applied.

*4. Man in the Middle attack*: The Man in the Middle Attack intercepts a malicious node between two communicating nodes which can be controlled by adversary in Fog. The malicious device can act as a middle device by eavesdropping between the nodes and identity information of the two normal devices when start communicating to store and forward all data. Whilst two nodes cannot detect the eavesdropper, instead they assume that they are communicating directly. The MITM Attack could breach the confidentiality, integrity and privacy of restricted data in Fog. The MITM attack can be instigated by simply depending on the protocols of communication which are used in Fog networks unlike any malicious node capture attacks where physical tampering with hardware of the devices is needed. Protocols of Secure communication and key management schemes are the efficient defense techniques to guard against these kinds of attacks and can ensure the identity.

*5. Routing Information attack*: In Routing Information Attacks, the adversary can manipulate the routing information and create route loops while transmitting the data over network there by leading the source paths extension and the raise of end-to-end delay in Fog networks. In Fog network, many of routing protocols used multiple links, switches and controllers for communication between the nodes and it ensures to protect the routing information. Trust management to constitute secure links among devices in Fog to make certain that the node identity information not to be seep out to the adversary.

*6. Sybil attacks*: Fog networks are large scale peer to peer networks, which has ability to compromise the malicious user. The malicious user is known as Sybil node has claimed multiple identifies to compromise the whole network. Sybil device has many valid identities; false data that was transmitted by the Sybil device can easily be received by their immediate neighboring devices. Interestingly, only a single path is determined and all the data that has been transmitted requires going through the Sybil device, in which jamming and DoS can be used. Secure identification and authentication mechanisms needed to be developed for Fog systems to defend against Sybil attacks.

*7. Unauthorized accesses*: In Fog, RFID is known to be an important enabling Technology and a most number of RFID tags are integrated. However, most of the authentication mechanisms are not support for RFID tags. Therefore the tags can be accessed and obtained to gain the information, modified and deleted by the adversary. Hence, it is a challenge for RFID-based devices to implement effective authorization access and authentication mechanisms and need further development.

*8. RFID cloning*: An attacker clones an RFID tag by copying data from the victims RFID tag, onto another RFID tag. Although the two RFID tags have identical data, this method does not reproduce the original ID of the RFID, making it possible to clone RFID and discern between the original and the compromised, unlike the event in the RFID spoofing attack.

*9. Traffic analysis attack:* The wireless characteristics of the RFID technology to inhale out the secret information or any other information by an attacker. Also, in almost all of the attacks an attacker first tries to gain some network information before he employs his attack. This is done using inhaling applications like port scrutinizing application, packet sniffer applications etc.

### 5.3 Application Level Attacks

These kinds of attacks mainly focused on the software which is used to support the services requested by the users. Software attacks are exploited the system by using Trojan horse programs, worms, viruses, spyware and malicious scripts which may pinch data, alter with information, deny the service and even harm the devices of a Fog system.

*1. Phishing attacks*: The adversary gain access to classified data of users such as user identification and password and authentication credentials of users through phishing websites and infected emails. Phishing attacks can be mitigating secure authentication, identification and authorization.

*2. Malicious virus/worms*: One of the most important challenges of Fog network/ application to infect with malicious software by an attacker. The malicious self propagation attacks like worms, virus, Trojan horses, Ransom ware, Spyware, etc., steeling information or tampering confidential data or even denial of service. In order combat with malicious software attacks in Fog applications, need the deployment of reliable anti software, detection of virus and other mechanisms of defensive are to be deployed.

## 6. Countermeasure for Security issues in Fog

In this part we will provide future directions and counter attacks for security mechanisms based on the classification presented earlier. A Fog network of IoT system consists of three different levels each with vulnerabilities and security attacks. To address these attacks and to successfully protect the Fog network in IoT system, this section presents a multi-level security approach that should be structured to give an optimal layered protection at each level in an Fog system as shown on the in Table1. A detailed description of the table is explained below.

*1. Device authentication*: To establish a fog network with the collection of nodes inter connected each other, when a new node is introduced to the network, it has to authenticate itself before receiving or transmitting data, to ensure it is identified correctly before authorization and keeping malicious devices out of the system. Various authentication mechanisms like PKI based authentication or DSS are used to authenticate the user identity such as digital certificates or certificate authorities.

*2. Data integrity*: Secure Hash Algorithm (SHA-1) can provide integrity service to Fog computing at each node. It ensures the data exchange between Fog nodes without modifications occurred on the sensitive data. We also study more secure cryptographic hash functions should be applied in Fog, which are used to calculate the hash value and verified at receiving node the only receive the data.

3. Data Confidentiality: Advanced Encryption Scheme (AES) should be used to encrypt the data to ensure confidentiality in Fog system. The encryption algorithms should be implemented with lower power consumption and less processing power. All RFID Tags, IDs and data should be encrypted on each device before transmission of data to ensure confidentiality. Strong encryption algorithms like ECDH, ECC are also implemented. Furthermore, various algorithms need to be implemented to provide the confidentiality to the node.

*4. Secure Booting*: Due to low computing and processing power of each node in the Fog network, software can be designed and implemented authentication and integrity mechanism. Most of the cryptographic algorithms need to be used ultra low power consumption devices.

*5. Anonymity*: The location privacy and identification of the node is anonym in Fog network. We study various approaches for this such as Zero-Knowledge approach would be the optimal solution for anonymity, it cannot be implemented on low power devices as it is a very strong algorithm and needs a lot of processing power; hence K- anonymity approach best fits the job for low power devices such as the devices used in a Fog system.

*6. Network security*: The security provided across the Fog network provides mainly three countermeasures, namely the schemes like identity authentication, data encryption and data integrity. Based these countermeasures including authentication and session key agreement, Group key agreement protocol is used to share the session keys among the nodes in Fog.

7. Routing security: In Fog network, secure routing is very important to the acceptance and use of sensor nodes for many Fog applications, but the conventional routing protocols are suitable. However, the dynamic environment provides multiple paths between the nodes to transmitted data. We study various routing algorithms to protect routing information but which improves their

performance and increase the security levels of routing data in Fog network.

*8. Data security*: In a Fog computing data security is more challenging since fog nodes that may collect the sensitive data concerning the identity and usage utilities. Moreover, fog nodes are scattered in large area, which is very difficult to centralized control. The compromise of a poorly secured edge node can be the entry point for an intruder to the network. The intruder once enters the network the steel the users' privacy data that is exchange among nodes. We need to implement cryptographic algorithms to protect from the unauthorized access to the system and ensures the confidentiality of the system data.

*9.Access Control Lists (ACLs):* Setting up policies and permissions of who can access and control the Fog system, is a crucial part as this ensures the privacy of the data, and the well being of the system. ACLs can block or allow the incoming or outgoing traffic, and give or block access to requests from different users inside or outside of the network.

*10 Firewalls*: This is an extra effective layer of security that will help block attacks that authentication, encryption and ACLs would failed to do so. Authentication and encryption passwords can be broken if weak passwords were selected. A firewall can filter packets in a way they are received, jams the unwanted packets, unfriendly login attempts, and DoS attacks before even authentication process begins.

*11Anti-virus, Anti-spyware and Anti-adware*: Security software like antivirus or anti spyware is important for the reliability, security, integrity and confidentiality of the Fog system.

## 7. Conclusion

We reviewed and analyzed security and privacy challenges and recent developments in Fog computing. We study several distinct characteristics of fog computing as well as a large scale of Fog devices at the edge of the network. In the direction of many research attempts security and privacy issues then require a reconfigurable Fog architecture for the applications that can multiple scenarios, Fog devices that allow storage, communication and computational resources to be efficiently used at the edge of the network .This study explores the various security goals required Fog environment and classified security attacks and their countermeasures based on the IoT architecture. We investigate the many papers to provide confidentiality, integrity and authentication services to implement trusted environment. Fog the Future directions, to implement trusted and security mechanisms to interact between the fog devices and provide secure communication over the fog network. We have presented security and privacy challenges and future directions to solve different challenges security and privacy in Fog computing.

## References

[1] Atzori, L., Iera, A., Morabito, G., 2010. "The internet of things: a survey". Comput. Netw. 54 (15), 2787–2805.

[2] D. Singh, G. Tripathi, and A.J. Jara. "A survey of Internet-of-things: Future vision, architecture, challenges and services." In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, pp. 287-292. IEEE, 2014.

[3] Yi, S., Hao, Z., Qin, Z., Li, Q., 2015a. "Fog computing: platform and applications". In: Proceedings of the Third IEEE Workshop on Hot Topics in Web Systems and Technologies, pp. 73–78.

[4] Veerraju T,Sai Ganesh S and Murthy GSN.," A study on Fog Computing based IoT: Security Issues and Challenges",Vol 6. Issue 12, pp.8257-8259. IJCAR, 2017.

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

[6] Sarkar, S., S. Chatterjee, and S. Misra. 2015. "Assessment of the suitability of fog computing in the context of internet of things". *IEEE Transactions on Cloud Computing* PP(99): 1–1.

[7] Varghese, B., N. Wang, S. Barbhuiya, P. Kilpatrick, and D.S. Nikolopoulos. 2016. "Challenges and opportunities in edge computing". In *Proceedings of the IEEE International Conference on Smart Cloud*, 20–26.

[8] D. Singh, G. Tripathi, and A.J. Jara. "A survey of Internet-of-things: Future vision, architecture, challenges and services." In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, pp. 287-292. IEEE, 2014.

[9] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3, pp. 648-651. IEEE, 2012.

[10] Redowan Mahmud, Ramamohanarao Kotagiri and Rajkumar Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions", Internet of Everything. Internet of Things (Technology, Communications and Computing), Springer 2017 103-130.

[11] Khan *et al. "*Fog computing security: a review of current applications and security solutions", *Journal of Cloud Computing: Advances, Systems and Applications* (2017) 6:19.

[12] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers, "Twenty security considerations for cloud-supported Internet of Things ",IEEE Internet of Things Journal ( Volume: 3, Issue: 3, June 2016 ), pp.269-284.

[13] Shanhe Yi, Zhengrui Qin, and Qun Li, "Security and Privacy Issues of Fog Computing: A Survey Wireless Algorithms, Systems, and Applications", LNCS 9204, Springer, 2015, pp. 685–695.

[14] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, Wei Zhao: "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications". IEEE Internet of Things Journal 4(5): 1125-1142 (2017)

[15] Mithun mukherjee, Rakesh matam et. al "Security and Privacy in Fog Computing: Challenges", 2169-3536 2017 IEEE. Translations and content mining are permitted for academic research only.