ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)

Vol. 5, Special Issue 9, March 2018

SECURITY ATTACKS IN FOG COMPUTING- BASIC CONCEPTS AND CHALLENGES

Jaya Prakash. S[1]
Assistant Professor, Dept. of Computer Science
Idhaya Engineering College for Women
Chinnasalem, India
sjpme1981@gmail.com

Vimaladevi.V[2]
Assistant Professor, Dept. of Computer Science
Idhaya Engineering College for Women
Chinnasalem, India
vimalamanii28@gmail.com

ABSTRACT

Fog computing is a new paradigm that extends the Cloud platform model by providing computing resources on theedges of a network. It can be described as a cloud-like platform having similar data, computation, storage andapplication services, but is fundamentally different in that it is decentralized. In addition, Fog systems are capable ofprocessing large amounts of data locally, operate on-premise, are fully portable, and can be installed onheterogeneous hardware. These features make the Fog platform highly suitable for time and location-sensitiveapplications. For example, Internet of Things (IoT) devices are required to quickly process a large amount of data. Thiswide range of functionality driven applications intensifies many security issues regarding data, virtualization, segregation, network, malware and monitoring. This paper gives an insight of theexisting security attacks that prevails in fog computing. This paper also determines the impact of those security issues and possible solutions, providing future security-relevant directions to those responsible for designing, developing, and maintaining Fog systems.

Keywords: Fog computing, Security threats, Internet of things, Performance, Wireless security, Malware protection

I.INTRODUCTION

Fog computing is a decentralized computing architecture whereby data is processed and stored between the source of origin and a cloud infrastructure. This results in the minimization of data transmission overheads, and subsequently, improves the performance of computing in Cloud platforms by reducing the requirement to process

and store large volumes of superfluous data. The Fog computing paradigmis largely motivated by a continuous increase in Internet of Things (IoT) devices, where an ever increasing amount of data (with respect to volume, variety, and velocity [1]) is generated from an ever expanding array of devices.IoT devices provide rich functionality, such as connectivity and the development of new functionality is oftendata motivated. These devices need computing resourcesto process the acquired data; however, fast decision processesare also required to maintain a high-level of functionality. This can present scalability and reliability issueswhen utilizing a standard client-server architecture, wheredata is sensed by the client and processed by the server. Ifa server was to become overloaded in traditional clientserverarchitecture, then many devices could be renderedunusable. The Fog paradigm aims to provide a scalabledecentralized solution for this issue. This is achieved bycreating a newhierarchically distributed and local platformbetween the Cloud system and end-user devices [2], as shown in Fig.

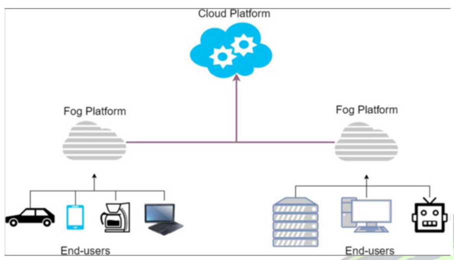
1. This platform is capable of filtering,aggregating, processing, analyzing and transmittingdata, and will result in saving time and communicationresources. This new paradigm is named *Fog computing*,initially and formally introduced by Cisco [3].Cloud computing

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)

Vol. 5, Special Issue 9, March 2018

provides many benefits to individualsand organizations through offering highly available andefficient computing resources with an affordable price [4].Many cloud services are available in current commercialsolutions, but they are not suitable for latency, portability



and location-sensitive applications, such as IoT, Wearablecomputing, Smart Grids, Connected Vehicles [5] andSoftware-Defined-Networks [6]. Latency depends on thespeed of Internet connection, resource contention amongguest virtual machines (VM) and has been shown toincrease with distance [7]. Furthermore, such applicationsgenerate large volumes of varied data in a high velocity,and by the time data reaches a cloud system for analysis,the chance to informthe IoT device to take reactive actionmay be gone. For example, consider IoT devices in themedical domain where the latency of acting on the senseddata could be life-critical.Cisco pioneered the delivery of the Fog computingmodel that extends and brings the Cloud platformcloser to end-user's device to resolve aforementionedissues. According to [8], a Fog system has the followingcharacteristics:

- It will be located at the edge of network with rich andheterogeneous end-user support;
- Provides support to a broad range of industrialapplications due to instant response capability.
- It has its own computing, storage, and networking Services.
- It will operate locally (single hop from device to Fog node).
- It is highly a virtualized platform; andOffers inexpensive, flexible and portable deploymentin terms of both hardware and software.Besides having these characteristics, a Fog system is differentfrom Cloud computing in various aspects and posesits own advantages and disadvantages. Some of the moreprominent are detailed in the below list [9–11].
- A Fog system will have relatively small computingresources (memory, processing and storage) when Compared to a Cloud system, but the resources can be increased on-demand.
- They are able to process data generated from a diverse set of devices.
- They can be both dense and sparsely distributed based on geographical location.
- They support Machine-to-Machine communication and wireless connectivity.
- It is possible for a Fog system to be installed on lowspecification devices like switches and IP cameras.
- One of their main uses is currently for mobile andportable devices.

II.SECURITY AND PRIVACY ISSUES IN FOG COMPUTING

A. TRUST

IoT networks are expected to provide reliable and secure services to the EUs. This requires all devices that are part of the fog network to have a certain level of trust on one another. Authentication plays a major role in establishing initial set of relations between IoT devices and fog nodes inthe network. But this is not sufficient as devices can alwaysmalfunction or are also susceptible to malicious attacks. In such a scenario, trust plays a major role in fostering relations based on previous interactions. Trust should play a two-way role in a fog network. That is, the fog nodes that offerservices to IoT devices should be able to validate whether thedevices requesting services are genuine. On the other hand,the IoT devices that send data and other valued processingrequests should be able to verify whether the intended fognodes are indeed secure. This requires a robust trust modelin place to ensure reliability and security in fog network.
Several works [14] have been carried out to address the issue of trust in cloud computing environment. However,the unique challenges posed by fog computing

environment necessitaterevisiting this problem. Contrary to cloud computing environment, the need for a fog node to quantify pastinteractions with IoT devices in the form of trust/reputationis to be addressed.

A. TRUST OF A FOG SERVICE*:*

A potential EU in fog computing needs to ensure trust-level provided by the fog serviceproviders. Therefore, it becomes necessary to answer .How do we measure trust in a fog service and whatare the main attributes that deny the trust of the fogservice?The well-established trust models in cloud computing canbe directly applied to fog computing due to lack of centralizedmanagement and mobility issues. Even though fog serviceprovider offers attributes to measure trust of a service, at thesame time, following question will arise asWho will verify and monitor these attributes?Among several trust-management model in cloud computing, reputation-based trust model is widely used ine-commerce services. Sometimes, reputation of a serviceprovider is useful to choose among several service providers.As this service model strongly depends on overall opinion,it is not well well-suited in fog computing due to dynamicnature of EU devices and fog nodes in the fog layers. In addition, although, opinion-based model is helpful to choose a fogservice, the reliability will become an important factor to beconsidered. Service Level Agreement (SLA) between a cloudservice and EU has gained a significant attention in designingtrust model in cloud computing. However, this SLA verification is limited when a user directly uses the cloud service,if the service is processed in the fog layer, a professional andlicensed third-party should monitor SLA verification for theEUs and small organization who lack in technical capability.

B. AUTHENTICATION

Authentication of networked devices subscribed to fog services is one of the foremost requirements in fog network.To access the services of a fog network, a device has to become part of the network by authenticating itself tothe fog network. This is essential to prevent the entry of unauthorized nodes. It becomes a formidable challenge asthe devices involved in the network are constrained in variousways including power, processing and storage. Traditionalauthentication mechanisms using certificates and Public-KeyInfrastructure (PKI) are not suitable due to the resource constraints of IoT devices. Alternatively, authentication protocolslike [27] have been proposed that is based on public-keyinfrastructure using multicast authentication for secure communications. In essence, like storage and processing services,authentication also needs to be offered as a service wherebya device that needs them would have to get authenticated tothe fog node with the help of the intermediary that may be theCertifying Authority (CA). This model of operations wouldprevent unauthorized nodes from becoming part of the fognetwork. In addition, this would also allow the fog nodes torestrict service requests from malicious/compromised nodes.

Dynamic fog nodes and EUs*:* Similar to mobility issue in EUs, the fog nodes also frequently join and leave the foglayer. It is required to ensure the uninterrupted service to theregistered end users when a new fog node joins (or leaves) thefog layer. The EU must be able to authenticate themselves tothe newly formed fog layer mutually. From EUs perspective,the complexity of registration and re-authentication phasewithout huge overhead.

C. SECURE COMMUNICATIONS IN FOG COMPUTING

The way processing and storage requirements can be offloaded to fog nodes, security requirements cannot be offloaded. Even IoT devices need to implement the minimumsecurity requirements. Communications between IoT devicesare considered to be taken care of the security practices inplace for IoT communications. IoT devices interact with fognodes only when they need to offer a processing or storagerequest. Any other interactions would not be considered aspart of the fog environment as such communications wouldhappen as part of the network. These fog nodes interact witheach other when they need to effectively manage networkresources or to

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)

Vol. 5, Special Issue 9, March 2018

manage network itself. They may even operatein distributed manner to perform a specific task. To securecommunications in a fog computing environment the following communications between these devices are to be secured:

1) communications between constrained-IoT devices andfog nodes and

2) communications between fog nodes.

Usually, an IoT device can initiate communication with any of the fog nodes in the fog network requesting for aprocessing or storage requirement. In fact the IoT devicemay not even be aware of the existence of the fog network,therefore messages sent by such a device cannot be securedby using symmetric cryptographic techniques. Alternatively,asymmetric key cryptography has its set of challenges thatare unique to IoT environment.

Maintaining the PKI thatis required to facilitate secure communication is one of themajor challenges. Other challenges include minimizing themessage overhead keeping in mind the constrained environment in which the IoT devices operate. Communications among fog nodes requires end-to-end security as nodesinvolved in multi-hop path may not be trust worthy.

D. END USER'S PRIVACY

Fog computing lies on the computational power of distributednodes for reducing the total pressure of the data center. In fogcomputing, privacy preservation is more challenging sincefog nodes that are in vicinity with EUs may collect sensitivedata concerning the identity, usage of utilities, e.g. smartgrid or location of end users compared to the remote cloudserver that lies in the core network. Moreover, since fog nodesare scattered in large areas, centralized control is becomingdifficult. The compromise of an poorly secured edge node canbe the entry point for an intruder to the network. The intruderonce inside the network can mine and steal users privacy datathat is exchanged among entities. Increased communication among the three layers that constitute the fog architecture canalso lead to privacy leakage.

Location privacy, as discussedin [15], is one of the most important models for privacy, sincethe place of equipment can be linked to the owners. Sincefog clients offload its tasks to nearest fog nodes, location, trajectory and even mobility habits can be revealed from anadversary. User habits can also be revealed from an adversaryby analyzing his/her usage habits of fog services, e.g. smartgrid. As shown in [16] smart meters' readings can discloseinformation about the time that the house is empty or eventhe TV programs that the EU prefers to watch.As new systems that are based on fog computing are pro-posed, new privacy challenges also arise. Ni *et al.* [12] propose the idea of Fog-based Vehicular Crowd Sensing (FVCS).In this system vehicular fog nodes can temporarily store andanalyze all sensing data that is uploaded by vehicles, in orderto provide local services, taking the role of central cloudservers. By exchanging data about local situation, e.g. trafficjam, each car can help in optimizing several parameters ofthe vehicle network, exposing on the same time sensitive dataabout their owners regarding their location, trajectory etc.

Theanonymization of the information and the tasks of differententities that need to be done for each task could put a heavy burden on pseudonym management for both customers andthe cloud [12].Even if systems are well designed and securely implemented, they can expose critical information through theirside channels. Possibilities of information leakage via sidechannels are pointed out in the literature and include electromagnetic radiation, observably timing of certain activities,power consumption of certain devices and even light acoustic or heat emanations from equipment [17]. All these privacyissues arise the need for more sophisticated solutions andcountermeasures.

E. MALICIOUS ATTACKS

Fog computing environment can be subjected to several malicious attacks and without proper security measures in placemay severely undermine the capabilities of the

network. Onesuch malicious attack that can be launched is a Denial-of-Service (DoS) attack. Since majority of the devices connectedto the networks are not mutually authenticated, launchinga DoS attack becomes straight forward. The attack may belaunched when devices that are connected to IoT networkrequest for innate processing/storage services. That is acompromised or malfunctioning node can make repeatedprocessing/storage requests to a fog node thereby stallingrequests made by legitimate devices. The intensity of such
an attack rises manifold when a set of nodes simultaneously launch this attack. Another way to launch this attackis to spoof addresses of multiple devices and send fakeprocessing/storage requests. Existing defense strategies ofother types of networks are not suited for fog computingenvironment mainly due to the openness of the network. Their major challenge is the size of the network. Potentially,hundreds and thousands of nodes forming an IoT networkavail the services of fog/cloud to overcome computation andstorage limitations and also enhance performance. Since allthese devices cannot be authenticated by fog nodes, they mayrely on trusted third party like a certification authority thatissues some form of credentials to ensure device authentication. But, the existence of such credentials only allows theprocessing fog node to verify whether the request has beengenerated by a legitimate node. Since a compromised nodeis a legitimate part of the network, all such requests wouldbe entertained. On the other hand, restricting connectivity tothe network or _altering the requests made by IoT devices nullify the motivation of existence of fog nodes. Spoofing
of addresses is also relatively easier as the address space is relatively large and lack of boundaries makes it even more difficult.

Malicious Insider to the cloud: One of the severe attacks to the cloud computing is the data theft attack by a maliciousinsider to the cloud provider. Basically, the end users have totrust on cloud service provider. Thus, lack of cloud provider'sauthentication results in data theft. Many incidents such asTwitter's personal and corporate data hacking [19], [20] andU.S. President Barack Obama's account hacking [39] revealthat the end user's password can be stolen effortlessly bya malicious insider. Rocha and Correia [40] discussed thatthe malicious insider to a cloud can easily get access to theuser data, however, end-users do not detect the unauthorizedaccess since the attack came from cloud service providerinside.Although many approaches are useful to secure data incloud computing using encryption and access control, misconfigured service, faulty implementation, bugs in coderestrict them to fully protect from sophisticated attacks . User behavior profiling can be useful to monitor the amountand duration of user data access. It can helps to detect theabnormal behavior of end-user, which can be further usedto predict the malicious attacks. Recently, Stolfo *et al.* [18]proposed a new level of security for the cloud. Based on the user behavior profiling, if the abnormal behavior is detected,then the decoy information is delivered to the true uses toobtain the response by many ways, e.g., security challenges.Otherwise, the decoy delivers a massive amount of garbagedata to the attackers, thereafter, reducing the stolen information of the users. At the same time following issues arise as:

_ Where to place the decoy in fog networks?

_ How to design on-demand decoy information to furtherreduce the amount of stolen data?

III. EXISTING RESEARCH IN FOG COMPUTING SECURITY AND PRIVACY

This Section summaries about the Existing research techniques in fog computing for the Security and privacy purpose of the Fog computing Users

A. FOG NETWORK SCALABILITY

The EU mobility, one of the main characteristics of fog computing, introduces many security and privacy issues in fog network. Moreover, fog nodes are very dynamic in natureas fog nodes join or leave the fog layer very frequently. Thewell-studied approaches in cloud computing are not directlyapplied due to several reasons. For example, although thetraditional PKI-based authentication is studied in thisapproach is not suitable to implement at the massive scale of fog node and EUs. Furthermore, password-based authentication is well-studied in cloud computing, however, it has many drawbacks as follows: 1) EUs are resourceconstraint, thus, extensive computation restricts the furtherimplementation at EU level and 2) since, the fog nodes usually collaborate among themselves, one common passworddoes not provide high security due to many attacks [55], such as vulnerability to off-line dictionary attack. Furthermore, theauthentication scheme based on Diffee-Hellman [56] keyexchange is not worthy due to slow and extensive modulocomputations.To address some of the above limitations, Ibrahim [32] proposed an efficient and secure authentication scheme thatallows any EU to authenticate with any fog Node mutually.Using this scheme, the randomly roaming EU authenticateswith any fog node that joins (or leaves) the fog layer very frequently, without a significant increase of overload. Thisfeature makes the scheme suitable for resource-constraintEUs devices.

The fog node (say, servers) in the fog layer is required to store only one secret key for each EU. TheEU stores the only one long-lived master secret key in theregistration phase. Using, this key, the EU mutually authenticates with any fog node managed by the cloud serviceprovider. Since a few hash invocations and symmetric keyencryption and decryption are required, it is suitable for amassive number of fog nodes and EUs without any PKI.

B. AUTHENTICATION AND PRIVACY-PRESERVINGSCHEMES FOR FOG COMPUTING

This part summarizes the authentication and privacy preserving schemes for fog computing. Hu *et al.* [42] proposed three schemes, namely, 1) identity authenticationscheme, 2) data encryption scheme, and 3) data integritychecking scheme, for fog computing with face identification and resolution application. Based on three maincountermeasures, including, authentication and session keyagreement, Advanced Encryption Standard (AES) symmetric key encryption mechanism based on session key, andSecure Hash Algorithm-1 (SHA-1), these three schemes can provide confidentiality, integrity, and availability underfog computing in IoT. Using Chinese remainder theorem,Lu *et al.* [21] introduced a Lightweight Privacy-preservingData Aggregation (LPDA) scheme, for fog computing-enhanced IoT. The LPDA can aggregate hybrid IoT devicesdata into one, as well as can resist against the false datainjection attack. In addition, the LPDA scheme is efficientin term of computational costs and communication overhead compared to the aggregation with the basic Paillier encryption, but the traceability is not considered. Wang *et al.* [23]introduced a differential privacy-based query model for sustainable fog computing supported data center. Using Laplacian mechanism, this query model is efficient in terms of execution efficiency, privacy preserving quality, data utility,and energy consumption compared with traditional privacypreserving models. To solve the privacy preserving issuefor the proximity detection in a fog computing system,Huo *et al.* [49] proposed a Location Difference-based Proximity Detection (LoDPD) protocol. Specifically, the LoDPDprotocol uses the Paillier encryption algorithm and decisiontree theory in order which can protect the privacy of theusers' location from disclosing to any party. Compared withthe Private Proximity Detection (PPD) protocol [50], the LoDPD protocol is efficient in term of the communicationcost. Supporting _ne-grained access control in a fog storagesystem can be considered as an important issue, as discussed in the work [17], where Koo and Hur proposed adeduplication scheme for encrypted data. Using user-levelkey management and update mechanisms, the scheme [17] can support regrained access control in a fog storage system. Compared to the scheme [46], the scheme [17] is efficient in terms of computation, communication, and storage,but the adversary model is limited. However, the uses ofthe fog computing paradigm can improve the effectiveness of certificate revocation distribution in IoT environments,as discussed in the work [20], where the authors proposeda scheme based on the four system entities, including, a CA, a back-end cloud, fog nodes, and IoT devices. In the boundedretrieval model,Yang *et al.* [47] proposed a secure positioningprotocol with location privacy for location-based fog computing. Xiao *et al.* [13] introduced a hybrid solution for engrained owner-enforced search in fog computing environment. Specifically, the scheme [13] is based on three mainphases, including,1) System initialization, 2) Sensitive data outsourcing storage, and 3) Search and access of outsourcedsensitive data.Fog-based vehicular crowdsensing is an emergingparadigm, as discussed by Ni *et al.* [12]. However, authentication and privacy-preserving are critical aspect related tothe functionality of crowdsensing reports. Basudan *et al.* [22] proposed a privacy-preserving scheme, called CertificateLess Aggregate SignCryption scheme (CLASC), for vehicular crowdsensing using fog computing. The CLASC schemecan achieve data confidentiality, integrity, mutual authentication, privacy, and anonymity. In addition, the CLASC scheme has the lowest computational cost compared to the existing schemes, but the location privacy is not considered.Similarly to the work [22], Liu *et al.* [45] introduced two secure traffic light control schemes in Vehicular Ad hoc Network (VANET) using fog computing. Based on twocountermeasures, namely, 1) Location based encryptionand 2) cryptographic puzzle, these two schemes areefficient to defending denial-of-service attacks, but theanonymity is not considered compared to the scheme [22]

and adversary's model is limited. Wang et al. [23] proposed a Dummy Rotation (DR) algorithm to ensure the anonymity on a fog structure for cloud location services. TheDR algorithm can achieve privacy-preserving by four privacy metrics, namely, 1) trajectory disclosure probability,2) position disclosure probability, 3) average Euclidean distance, and 4) local data volume. Similarly to the scheme [21],Wang *et al.* [24] proposed an aggregation scheme in fogbased public cloud computing, called anonymous and secureaggregation scheme (ASAS). Specifically, the ASAS schemeconsiders a fog-based public cloud computing with four typesof entities, including, system manager, terminal devices,a fog node, and a public cloud server. Based on two maincountermeasures, namely, 1) Elliptic curve public-key cryptography and 2) Castagnos Laguillaumie cryptosystem, theASAS can preserve the anonymity and identity privacy, butthe adversary's model is limited.

C. FOG FORENSICS

The cloud forensic [57] provides the digital evidenceby reconstructing past cloud computing events. Basically,it has the challenges in three dimensions as follows [57]:

1) ***Technical dimension***includes the inaccessibility to brain*log data* from the cloud, volatile data, integrity and correctness of the data, and multi-tenancy,
2) ***Organizationaldimension***refers to lack of forensics experts, in addition,
3) ***Legal dimension***focuses on customer awareness, Internetregulation, and cross-border law. Few steps are already takento overcome some of these above issues. For example, Biggsand Vidalis [34] and Wolthusen [35] considered global unityto overcome the cross-border issue. Moreover, a continuoussynchronization [58] was suggested to handle volatile data

Furthermore, the isolation of cloud instances [59] is proposedto overcome the multi-tenancy issues.Followed by cloud forensic, fog forensic is defined as theapplication of digital forensics in fog computing. As observedby Wang *et al.* [24], fog forensics that has some stepssimilar to cloud forensic, however, is not a part of cloudforensics.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)

Vol. 5, Special Issue 9, March 2018

Although some challenges in fog forensics aresame as cloud forensics (e.g., cyber-physical systems andcustody chain dependency, and integrity preservation), manychallenges are more significant in fog forensics compared tocloud forensics. For example, since fog computing consistsof massive number of fog nodes as infrastructure, retrievingthe log datafrom these fog nodes becomes very difficult.Nevertheless, fog computing is geographically distributed,thus the cross-border issue is less critical compared to thecentralized cloud forensics. However, due to a large numberof fog nodes, the dependability issue becomes more crucialin fog forensics.

IV. OPEN QUESTIONS AND RESEARCH CHALLENGES

The cloud computing is generally heavily protected by cloudoperators, nevertheless, all of the security solutions cannot be easily extended to fog computing due to many reasons. Although a few works, such as [16], [12], [17], [23], considered the secure interaction of fog elements, authentication, and authorization for the fog computing, intruder detection, key agreements for fog computing, theseapproaches are either partially addressed the security andprivacy issues or still in very early stages. This section outlines the open research challenges in fog security and privacyissues. Fig. 2 illustrates some of the open research challengesin fog privacy and security issues.

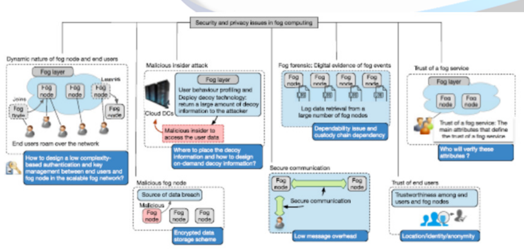


FIGURE 2. Open research challenges in fog security and privacy issues.

A. TRUST

Addressing issues related to trust in a fog network is slightlytrickier compared to cloud computing environment. Theopenness of fog computing environment and the two-wayrequirement of trust are major challenges in designing a trustmodel for fog network. In other words, cloud computingenvironment have an in place security infrastructure adhering to security standards of the industry that allows EUsand businesses to develop a level of trust over the cloud.On the other hand, this is absent in FogNet that makes itmore open and vulnerable to security attacks. Even thougha common security framework can be employed by all the

fog nodes forming the FogNet, high dynamism makes it challenging in addressing the issue of trust. In addition, trust istwo-way requirement in FogNet but it is more-or-less unidirectional in cloud computing. Businesses and end userssubscribing to cloud can quantify trust relationships andany malicious activity of end users can be defended using firewalls, intrusion detection systems and other securitypractices.But, in a FogNet the fog nodes also need tomaintain trust relations with the devices using fog net-work services. Also, the IoT devices that entrust fog nodeswith data and processing requests need to develop trustedinteractions with the fog nodes. This two-way challengein FogNet makes the design of trust model a formidablechallenge.

B. PRIVACY PRESERVATION

As resources of EU's devices are shared among other geographically close devices to support context-aware services [63], location, massive amount data and otherinformation of EU need to be protected in very secure manner. As an use-case scenario, in [33], where a UnmannedAerial Vehicles (UAVs)-based integrative IoT platform forintegrating UAVs into the fog computing is suggested,the attackers through communication attacks such as theMan-In-The-Middle (MITM) attack easily exploit this platform to disclose sensitive information such as location andidentity of the fog nodes. Therefore,

C. AUTHENTICATION AND KEY AGREEMENT

Authentication at different level of gateways is one of the major concern in fog computing where fog nodes are acting as data aggregation and control point of data collectedfrom resource-constraint devices. Thus, a lightweight aswell as end-to-end authentication is equally

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)

Vol. 5, Special Issue 9, March 2018

important in thiscontext. For example, in fog computing-based radio access networks (F-RANs) [36], which is adaptive to the dynamic traffic and radio environment, how to achieve scalable,authentication and billing in the context of F-RANs is oneof the most important issues. Hence,the authentication and key agreement protocols for F-RANs are major challenges and should be exploitedin the future.In addition, user-level key management and

updatemechanisms to support fine-grained access control in afog storage system is an important task.

D. INTRUSION DETECTION SYSTEMS

Intrusion Detection methods are widely used nowadays in order to mitigate attacks such as scanning attacks, dos attacks,insider attacks or MITM attacks and can be applied to different systems, e.g. SCADA [25], cloud [26], smart grid [27]etc. In fog computing IDS must be deployed in a all thelevels of the three tier architecture monitoring and analyzing traffic and behavior of fog nodes, end devices and cloudservers. Securing one level of the system is not enough toguarantee that a virus or malware will not propagate froma vulnerable node to the rest of the system. By deployingIDS mechanisms to each level of a fog computing, challenges like real time notification, alarm parallelization, false alarmcontrol and correct response arise [68]. A deployment of aperimeter Intrusion Detection System that can coordinate them different detection components that will be spread inside thefog system is needed.

E. DYNAMIC JOIN AND LEAVE OF FOG NODE

Since the fog node leaves or joins a fog layer very frequently,critical security issues arise as follows:How to handle the security and privacy issues when aFog node joins or leaves the fog layer? For example, howthe EUs authenticate themselves to the new fog node andhow the privacy of the EUs can be preserved when a Fognode leaves the fog layer? How to design a low complexity-based authenticationbetween EU and fog node in the scalable fog network?How to keep the anonymity of the users and to trace theusers with their true identity once user misbehavior isdetected by the cloud service provider?

F. CROSS-BORDER ISSUE AND FOG FORENSIC

Although the cross-border issue is less significant as compared to cloud computing due to distributed nature of fog computing, the fog forensics still require international legislation and jurisdictions [18], [19] and application levellogging. Therefore, it is still an important task to overcome cross-border legislation challenges in fog computing.

V. CONCLUSION

Security and privacy issues are well-studied in cloud computing, however, all of them are not suitable for fog computingdue to several distinct characteristics of fog computing as wellas a wider scale of fog devices at the edge of the network.In addition, many new security and privacy threats arisethat were not presented in centrally managed cloud computing.In this article, we have presented an overviewof main securityand privacy issues in fog computing. Afterward, this paperdeals with the state-of-the-art to deal with the fog computingrelated security and privacy challenges. In summary, the aimof this paper is to summarize up-to-date research contributions and to outline future research direction to solve differentchallenges in privacy and security in the fog computing.

REFERENCES

[1] Sagiroglu S, Sinanc D (2013) Big data: A review. In Collaboration Technologies and Systems (CTS), 2013 International Conference On IEEE. pp 42–47

[2] Cisco (2015) Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are.Online:https://www.cisco.com/c/dam/enus/solutions/trends/iot/docs/computing/solutions.pdf. Accessed 13 Dec 2016

[3] Tang B, Chen Z, Hefferman G, Wei T, He H, Yang Q (2015) A hierarchical distributed fog computing architecture for big data analysis in smart cities. In:

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)

Vol. 5, Special Issue 9, March 2018

Proceedings of the ASE BigData & SocialInformatics 2015. ACM. p 28

[4] Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A (2011) Cloud computing-the business perspective. Decis Support Syst 51(1):176–189

[5] Parkinson S, Ward P, Wilson K, Miller J (2017) Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans Intell Transp Syst PP(99):1–18. doi:10.1109/TITS.2017.2665968

[6] Stojmenovic I, Wen S (2014) The fog computing paradigm: Scenarios and security issues. In: Computer Science and Information Systems (FedCSIS), 2014 Federated Conference On. IEEE. pp 1–8

[7] Kim JY, Schulzrinne H (2013) Cloud support for latency-sensitive telephony applications. In: Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference On, vol. 1. IEEE. pp 421–426

[8] Bonomi F, Milito R, Zhu J, Addepalli S (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. pp 13–16

[9] Sareen P, Kumar P (2016) The fog computing paradigm. Int J Emerging Technol Eng Res 4:55–60

[10] Vaquero LM, Rodero-Merino L (2014) Finding your way in the fog: Towards a comprehensive definition of fog computing. ACM SIGCOMM Comput Commun Rev 44(5):27–32

[11] Saharan K, Kumar A (2015) Fog in comparison to cloud: A survey. Int J Comput Appl 122(3):10–12

[12] J. Ni, A. Zhang, X. Lin, and X. S. Shen, ``Security, privacy, and fairness in fog-based vehicular crowdsensing," IEEE Commun. Mag., vol. 55, no. 6, pp. 146_152, Jun. 2017.

[13] M. Xiao, J. Zhou, X. Liu, and M. Jiang, ``A hybrid scheme for fine-grained search and access authorization in fog computing environment," Sensors, vol. 17, no. 6, pp. 1_22, Jun. 2017.

[14] R. K. L. Ko et al., ``TrustCloud: A framework for accountability and trust in cloud computing," in Proc. IEEE World Congr. Services, Jul. 2011, pp. 584_588

[15] M. A. Ferrag, L. Maglaras, and A. Ahmim, ``Privacy-preserving schemes for ad hoc social networks: A survey," IEEE Commun. Surveys Tuts., to be published.

[16] Y. Hong, W. M. Liu, and L. Wang, ``Privacy preserving smart meter streaming against information leakage of appliance status," IEEE Trans.Inf. Forensics Security, vol. 12, no. 9, pp. 2227_2241, Sep. 2017.

[17] D. Koo and J. Hur, ``Privacy-preserving deduplication of encrypted data with dynamic ownership management in fog computing," Future Generate Comput. Syst., to be published