Privacy and Security Problems in Fog Computing

Article · March 2016

DOI: 10.5120/cae2016652088

Khalid A. Fakieh
King Abdulaziz University

Privacy and Security Problems in Fog Computing

Khalid A. Fakeeh, PhD
FCIT,
King Abdul-Aziz University,
Jeddah, Saudi Arabia

ABSTRACT

Fog Computing is a term made by Cisco that insinuates extending cloud computing to the edge of a network. Generally called Edge Computing or preliminaries, fog computing supports the operation of Fog/cloud, storage and networking services between end devices and conveyed processing data centers. Fog computing is a gifted computing perspective that extends cloud computing to the edge of frameworks/networks. Like cloud computing however with specific characteristics, fog computing faces new-fangled security and assurance defies other than those procured from cloud computing. We have reviewed these defies/concerns and prospective plans briefly in this paper.

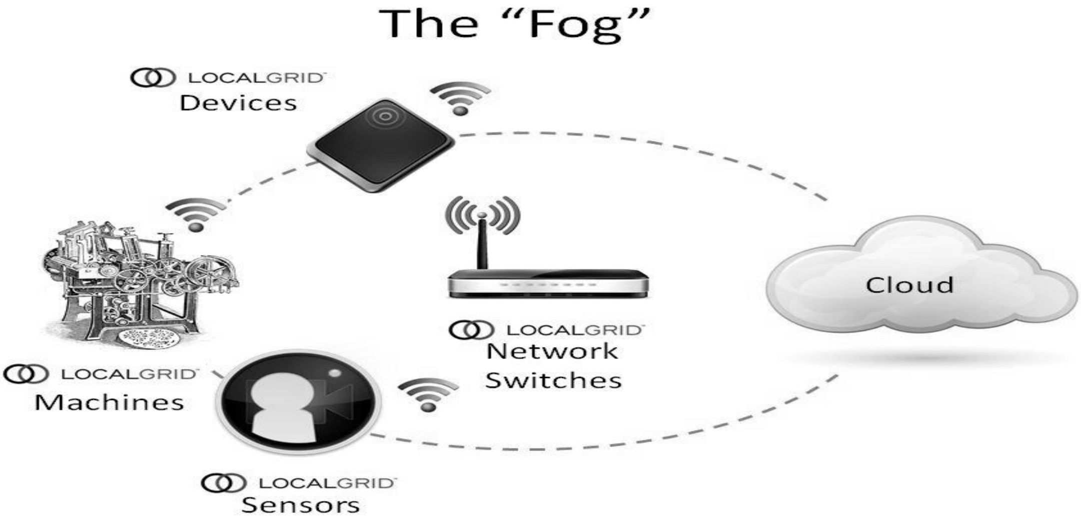
Keywords

Cloud computing, Fog computing, IoT, Security, Confidentiality

1. INTRODUCTION

The pervasiveness of all around joined astute or smart devices are framing the computer principal aspect. Quick headways of wearable computing, smart home/city, and smart meters connected vehicles and generous scale remote sensor networks are making everything related and all the more clever, termed the Internet of Things (IoT). International Data Corporation (IDC) has expected that in the year of 2015, the IoT will continue to rapidly amplify the standard IT industry up 14 percent from last year [Gil Press 2015]. As we likely are mindful, smart devices generally confront problems or issues arises from battery, computational processes, bandwidth and storage so called a big hindrance for Quality of service and customer

Experience and practice. To diminish the heaviness of restricted resources on smart devices, cloud computing is considered as a promising computing perspective, which can pass on services to end customers in regards to platform & programming, infrastructure, and supply applications with adaptable resources effectively. Cloud computing, regardless, is not a versatile game plan or way out. There are still issues up in the air since IoT applications by and large require flexible mobility hold up, geo-distribution, location awareness and low torpidity or latency. Fog computing is projected to enable computing particularly at the edge of the framework/network, which can pass on novel applications and services for billions of joined devices [Bonomi et al]. Set-top-boxes, access points, road side units, cellular base stations, et cetera are usually Fog devices. End devices, cloud and fog are confining a three layer different leveled service delivery model, supporting an extent of usages, for instance, web content transport [Zhu et al, 2013], augmented reality [Ha et al, 2014], and immense data examination [Zao et al, 2014]. A regular hypothetical architecture of fog or cloud is depicted in Fig 1 (a, b, c).



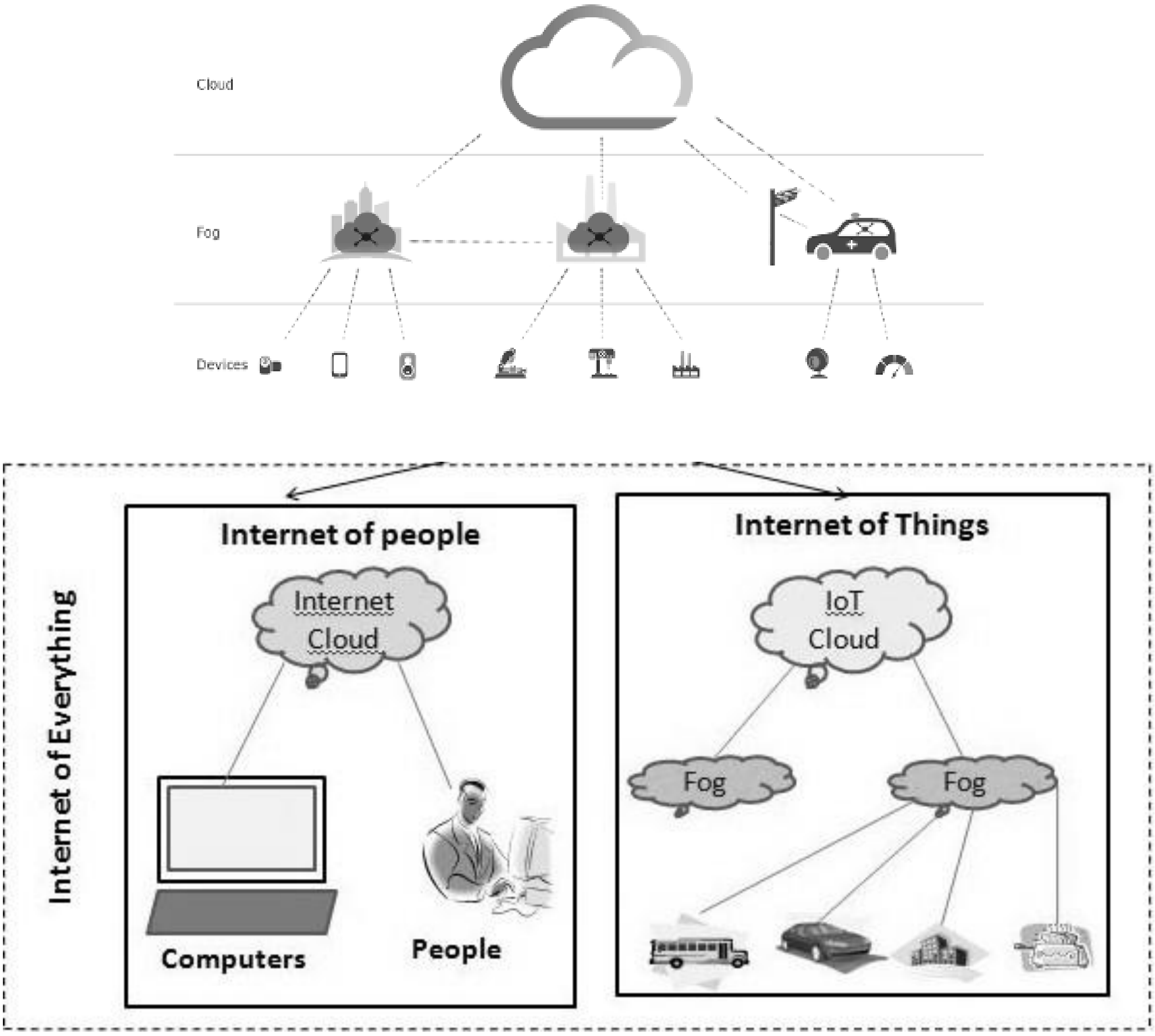


Fig 1 (a) (b) (c): Fog Architecture

Since Fog is viewed as a non-piddling development of cloud, some security and insurance/privacy issues or defies in the association of Cloud Computing (CC) [Takabi et al, 2010], can be anticipated to inescapably impact fog computing. And such concerns issues will slack the progression of fog computing if not all that much tended to, according to the way that seventy-four percent of IT Executives and CIO's reject cloud in term of the perils in privacy and security [Zissis et al, 2012]. As fog computing is still in its infant stage, there is little work on above issues. In view of the fact that fog computing is planned in the setting of Internet of Things (IoT), and started from cloud computing, above mentioned issues of cloud are gained in fog computing. While a couple concerns can be had a tendency to exhausting on hand arrangements, there are diverse problems going up against new troubles, as a result of the specific properties of fog computing, for instance, fog's node heterogeneity and fog framework/network, essential of low power, mobility hold up, gigantic scale geo-scattered center points location awareness.

2. GENERAL IDEA OF FOG COMPUTING:

For brief surveys readers can go for [Zhang et al 2010, Dinh et al 2013] if fascinated. Being a new paradigm fog computing is still not publicly a versatile concept. Fog computing is considered as a development of the cloud computing to the edge of the framework/network, which is an extremely virtualized phase or platform of resource collection that bestows computation, storage, and networking services to end customers as depicted in Fig 2.

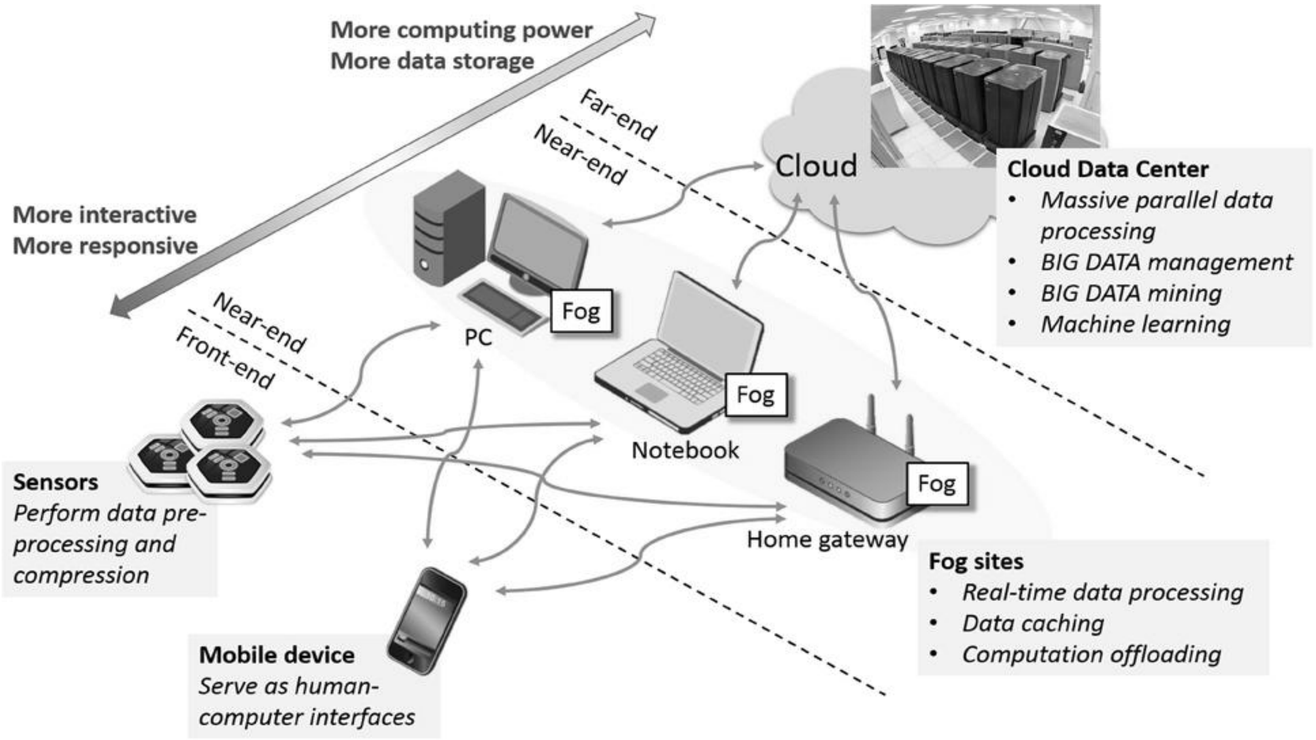


Fig 2: Fog Computing Overview

In light of [Vaquero et al, 2014], they have classified “fog computing as a circumstance where a tremendous number of heterogeneous ubiquitous and decentralized devices communicate and perhaps take an interest among them and with the framework/network to perform storage and processing errands devoid of the intervention of third-parties. These assignments can be for sustaining principal limitations of network or fresh applications and services that continue running in a sandboxed milieu. Customers leasing some bit of their devices to have these services get persuading strengths for doing all things considered”. Fog computing has its central focuses or pros as a result of its edge location, and thusly can reinforce applications such as expanded reality, gaming, consistent video stream with small idleness or latency rations. This edge territory can in like manner bestow rich framework/network association information, for instance, close-by network milieu, traffic data figures and client status information, which can be brought into play by fog applications to bestow context-aware progression. Location awareness is an another appealing trademark; not simply can the geo-scattered fog center points or nodes determine its own zone also the fog node can track the devices of end customer to reinforce flexibility, which may be an entertainment changing component for zone/location based applications and services. Additionally, the trades amidst cloud and fog, fog and fog get the opportunity to be basic in view of the fact that fog can devoid of a lot of a stretch get neighborhood graph despite the fact that the overall coverage can only be pulled off at higher layer. As far as fog nodes are concern so the inescapability of smart devices and quick progression of standard virtualization and cloud advancement make multi fog nodes execution advantage competent. A kind of fog nodes which is commonly in view of existing network devices are called “resource poor fog nodes”. A novel fog computing architecture named as ParaDrop in [Willis et al, 2014] is another fog computing paradigm on gateway, which is an impeccable fog node choice on account of its capacities to confer service and its proximity at network edge. Since the usual home environment sections are resource confined, the authors put into practice the ParaDrop exercising Linux Container (LXC) idea which is more lightweight than standard virtual machines. On the other hand the Resource rich fog nodes are for the most part stipulated awesome servers with fit CPU, greater memory and aptitude. Cloudlet [Satyanarayanan et al 2009 & 2015], like a second-class data center can give flexible advantages for near to mobile devices, with low latency and far reaching transmission qualifications. With cloud methods, Cloudlet is definitely not hard to overhaul/upgrade and supplant. Now if look upon the service delivery and deployment models, so similar to cloud computing, it can be expected that the service delivery models in fog computing can be assembled into three characterizations: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). As far as deployment models are concern so we may similarly expect these as private fog, public fog, community fog and hybrid cloud. Now let’s come to next terms which are Mobile cloud computing (MCC) and Mobile edge computing (MEC) are comparable to fog computing. Mobile cloud computing implies a base in which both the data storage and the data processing come about outside of the mobile phones [Dinh et al, 2013]. Mobile edge computing focus on resource rich fog servers like cloudlets running at the edge of adaptable networks/frameworks [ETSI, 2014]. Fog computing isolates itself as a more summed up computing perspective especially in the association of Internet of Things (IoT).

3. PROBLEMS OF SECURITY & PRIVACY:

It has been acknowledged that security and privacy should be tended to in every layer in building fog computing system. Below are defies or problems, which may possibly have need of future work to overcome.

3.1 Reliance and Authentication/Verification:

Data centers are commonly controlled by cloud service suppliers in Cloud Computing (CC) deployment or operation. In any case, fog service suppliers can be unusual parties as a result of diverse deployment choices: i) Internet service suppliers or wireless careers, who have control of home gateways or cellular base stations, may put up fog with their on hand infrastructures. ii) Cloud services suppliers, who need to extend their cloud services to the edge of the framework/network, may in like manner build fog infrastructures; iii) End customers, who have a close-by private cloud and need to diminish the cost of proprietorship, might need to change the local private cloud into fog and rent auxiliary resources on the local private cloud. This suppleness set hurdles for the fog trust provision. Reputation based trust model [J sang et al, 2007] has been compelling in customer reviews and online social networks, E-commerce, peer-to-peer (P2P). The [Damiani et al, 2002] planned an in number reputation structure for resource determination in P2P frameworks/networks exercising a scattered or distributed polling computation (algorithm) to assess the immovable nature of a resource prior to downloading. In sketching out a fog computing reputation based reputation structure, it may possibly need to grip problems such as how to pull off tenacious, distinctive, and specific character/uniqueness, and how to treat deliberate and accidental misbehavior, and also how to demeanor retribution and recuperation of reputation. There are moreover trusting models in light of excellent hardware, for instance, Trusted Platform Module (TPM), Trusted Execution Environment (TEE) or Secure Element (SE) which can bestow trust utility in applications of fog computing. Regarding rogue fog node so a rogue fog node would be a fog device or fog case that puts on a show to be completely forthright to goodness and urges end customers to join with it. For instance, in an insider strike, a fog executive may be affirmed to administer fog events, yet may instantiate a nonconformist fog sample instead of a genuine one. A [Stojmenovic et al, 2014] has confirmed the achievability of man-in-the-inside attack in fog computing, before which the gateway should be either exchanged off or supplanted by a fake one. Once related, the adversary can control the drawing closer and dynamic sales from end customers or cloud, accumulate or adjust customer data stealthily, and adequately dispatch further strikes. The fake fog node existence will be a striking jeopardy to security and privacy of customer data. This concern is hard to address in fog computing in view of such reasons such that complex trust situation calls for dissimilar trust management methods and vibrant construction and erasure of virtual machine instance make it hard to keep up a blacklist of rogue nodes. Authors of [Han et al, 2009 & 2011] have projected an estimation based method to facilitate a customer to pass up connecting rogue access point. Their technique impacts the round-trip time between DNS server and end customers to recognize rogue access point at the customer region. Authentication or verification is a basic concern for the security of fog computing in view of the fact that services are put forward to massive scale end customers by front fog nodes. Authors of [Stojmenovic et al, 2014] have well thought-out the essential security concern of fog computing as the affirmation at diverse levels of fog nodes. Ordinary PKI-based verification or authentication is not resourceful and has underprivileged suppleness. The [Balfanz et al, 2002] have anticipated a shabby, sheltered and straightforward response for the authentication concern in close-by uncommonly selected remote framework/network, contingent upon a physical contact for pre-check in a range obliged channel. Basically, NFC can similarly be brought into play to enhance the confirmation or authentication system because of cloudlet [Bouzefrane et al, 2014]. As the ascent of biometric check in cloud and mobile computing, for instance, verification and in fog computing it will be favorable to apply biometric-based verification in it.

3.2 Network fortification:

In view of the greatness of wireless networking in fog computing, remote framework or wireless network security is colossal stress to fog computing. Attacks or strikes like jamming, sniffing can be tended to in the examination range of wireless networks. Commonly, in network, it is something has to trust the configurations manually delivered by a framework/network manager and detach network management traffic from general data traffic [Tsugawa et al, 2014]. Nevertheless, fog nodes are sent at the edge of Internet, which definitely pass on overpowering load to the network management, imagining the cost of keeping up massive scale cloud servers which are scattered all around all through the framework/network edge without basic access for upkeep. The control of software defined networks can encourage the execution and management, and fabricate adaptability of network and lessening expenses, in various parts of fog computing. It also should not be left mentioned that applying SDN technique in fog computing will get fog computing security novel defies and prospects. In what way can SDN put forward the fog some help with network security?

- CloudWatch [Shin et al, 2012] can impact OpenFLow [McKeown et al, 2008] to course traffic for security watching applications or Intrusion Detection System.
- Traffic Isolation and Prioritization can be brought in to play to keep an ambush from stopping up the framework/network or directing shared resources, for instance, CPU or disk I/O. SDN can without a doubt make use of VLAN ID/tag to independent traffic in VLAN assembling and confine poisonous traffic.
- Authors of [Klaedtke et al, 2014] have projected an access control arrangement on a SDN controller considering OpenFlow.
- Fog updated router in home framework/network can be opened to guests, if the network granting to guests is intentionally expected to security concerns. Authors in [Yap et al, 2011] have projected OpenWiFi, in which the guest WiFi verification is moved to the cloud to set up guest character; access is autonomously obliged guests; and accounting is approved to choose guests liability.

3.3 Safe & Protected Data Storage & Computation

In Fog computing, customer data is outsourced and customer's control over data is offered over to fog node, which exhibits identical security perils as it is in cloud computing (CC). To begin with, it is hard to ensure data uprightness, in view of the fact that the outsourced data could be lost or mistakenly tailored. Subsequent, the exchanged data could be abused by unapproved parties for diverse side wellbeing's. To address these perils, auditable data storage service has been anticipated in the setting of cloud computing to guarantee the data. Strategies, for instance, searchable or homomorphic encryption are joined to bestow uprightness, privacy and verifiability for cloud storage structure/system to permit a client to test out its data set away on untrusted servers. The [Wang et al, 2010] have projected privacy-preserving public auditing for data set away in cloud, which relies on upon a third party auditor (TPA), by means of homomorphic authenticator and self-assertive or random mask method to guarantee assurance against TPA. To ensure data storage immovable quality, previous storage structures bring into play erasure codes or framework/network coding to oversee data sleaze recognizable proof and data repair, while the authors of [Cao et al, 2012] have wished-for an arrangement exercising LT code, which bestows less limit cost, much speedier data recuperation, and comparative correspondence cost. The [Yang et al, 2012] have given a tolerable survey of existing work in cloud computing towards data storage auditing services. There are new-fangled troubles in arranging secure storage system to pull off low latency, support dynamic operation and oversee trade amidst cloud and fog. Another basic issue in fog computing is to pull off safe and sheltered computation outsourced to fog nodes. Verifiable Computing facilitates a computing device to pass on the computation of ability to diverse possibly untrusted servers, while keeping up verifiable gifted outcomes. Substitute servers evaluate the limit and give back the result with a proof that the computation of the limit was did precisely. [Gennaro et al, 2010] Has formalized verifiable computing. In fog computing, to imbue confidence in the estimation offloaded to the fog node, the fog customer should have the ability to check the computation exactness. The accompanying are some present procedures to fulfill verifiable computing. Authors of [Gennaro et al, 2010] have planned a verifiable computing protocol that facilitates the server to give back a computationally-stable, non-interactive confirmation that can be verified by the client. The protocol can give information and yield assurance for the client such that the server does not appreciate any information about the data and yield/output. Parno and Gentry have made a system, called Pinocchio, such that the client can check general estimations done by a server while depending just on cryptographic suppositions [Parno et al, 2013]. With Pinocchio, the client makes an open appraisal key to depict her count or computation, and the server then evaluates the computation and brings into play the appraisal key to convey a proof of rightness. To guarantee data security, fragile data from end customers must be encoded before outsourced to the fog node, making efficient data deployment services testing. A champion amongst the most basic services is keyword search, keyword look among encrypted data files. Masters have added to a couple of searchable encryption plots that allow a customer to securely look for over encrypted data through keywords devoid of unscrambling. The authors of [Song et al, 2000] anticipated the opening scheme for rummages around on encoded data, which bestows incontestable riddle to encryption, query repression/isolation, controlled searching, and hidden query hold up. Various distinctive arrangements such as [Wang et al 2012, Cash et al 2014] have been created later on.

3.4 Confidentiality or Privacy

The spillage of confidential information, for instance, data, zone/location or deployment, are getting contemplations when end customers are putting into practice services such as IoT, WSN, cloud computing. There are also defies for ensuring such security in fog computing, in light of the fact that fog nodes are in of end customers locality and can assemble more fragile in-plan than the remote cloud lying in the middle framework/network. Privacy-preserving methodologies have been planned in various circumstances together with cloud [Cao et al, 2014], online social networks [Novak et al, 2014], wireless network [Qin et al, 2014] and smart grid [Rial et al, 2011]. In the fog network, Privacy-preserving methodologies can be running amidst the fog and cloud while those computations are normally resource denied toward the end contraptions or devices. Fog node at the edge generally assembles sensitive data delivered by sensors and end contraptions/devices. Methods, for instance, homomorphic encryption can be exploited to allocate privacy-preserving aggregation at the area doors devoid of unscrambling [Lu et al, 2012]. Differential confidentiality or privacy [Dwork, 2011] can be brought into play to ensure non-disclosure of confidentiality of a subjective single section in the data set if there ought to emerge an event of quantifiable queries. One more security concern is the employment outline with which a fog client makes use of the fog services. Case in point in smart grid, the scrutinizing of the smart meter will reveal piles of information of a family unit, for instance, at what time there is no person at home, and at what time the TV is turned on, which entirely breaks customer's privacy. Regardless of the way that privacy-preserving methodologies instrument have been projected in smart metering [McLaughlin et al, Rial et al, 2011,], they can't be joined in fog computing particularly, as a result of the nonattendance of a trusted pariah or third party or no accomplice contraption/device like a battery. The fog node which can devoid of quite a bit of a stretch accumulate estimations of end customer practice or usage. One possible gullible course of action is that the fog client makes sham assignments and offloads them to diverse fog nodes, disguising its bona fide endeavors among the fake ones. Then again, this game plan will extend the fog client's cost and waste resources and imperativeness or energy. Another course of action would be arranging a sharp strategy for separating the application to guarantee the offloaded resource utilizations don't divulge confidential information. In fog computing, the territory security mainly implies the zone assurance of the fog clients. As a fog client generally speaking offloads its endeavors to the nearest fog node, the fog node, to which the errands are offloaded, can derive that the fog client is contiguous and more far off from distinctive nodes. In addition, if a fog client makes use of different fog services at diverse ranges, it may reveal its path heading to the fog nodes, tolerating the fog nodes interest. For whatever period of time that such a fog client is attached on an object or whatever it to, the location privacy of the individual or the thing is at threat. In case a fog client constantly altogether picks its nearest fog server, the fog node can unquestionably understand that the fog client that is exercising its preparing resources is adjoining. The most ideal approach to ensure the region security or privacy is through character/identity tangling such that in spite of the way that the fog nodes knows a fog client is adjoining it can't recognize the fog client. There are various systems for identity jumbling; for example, authors of [Wei et al, 2012] bring into play a trusted outcast to create fake ID for each end customer. In reality, a fog client does not as per usual pick the nearest fog node yet rather picks openly one of the fog nodes it can get to concurring some criteria, for instance, idleness, load balance standing, etc. For this circumstance, the fog node can simply know the repulsive territory of the fog client yet can't do all things considered specifically. Regardless, once the fog client brings into play computing resources from various fog nodes in an extent, its region can come down to a little region, since its region must be in the intersection purpose of the different fog nodes coverage's or ranges. By bringing into play procedure of [Gao et al, 2013] we can preserve the region security in such circumstances.

3.5 Access Control

As far as Access control is concern so it has been a tried and true gadget to ensure the security of the structure and securing of assurance of customer. Standard access control is ordinarily tended to in a same trust region. While due to the outsource method for cloud computing, the access control in cloud computing is by and large cryptographically realized for outsourced data. Symmetric key based course of action is not versatile in key management. A couple open key based courses of action are proposed endeavoring to fulfill fine-grained access control. Authors of [Yu et al, 2010] have planned a fine-grained data access control arrangement created on attribute-based encryption (ABE). Authors of [Dsouza et al, 2014] put forward a policy-based resource access control in fog computing, to support secure joint exertion and interoperability between heterogeneous resources. In fog computing, how to arrange access control crossing client fog cloud, meanwhile meet the arranging goals and resource constrictions will be frustrating.

3.6 Intrusion Detection (ID)

As far as ID is concern so its methodologies are comprehensively passed on in cloud structure to reduce molests, for instance, insider ambush, attacks on VM and hypervisor, flooding strike, port checking etc [Modi et al, 2013], or in smart grid system to screen smart-meter measurements and distinguishes sporadic estimations that could have been bartered by aggressors [Valenzuela et al & Qin et al, 2013]. In fog computing, IDS can be sent on fog node system side to recognize sniffing activities by observing and scrutinizing, access control methodologies, log files and customer login information. They can in like manner be sent at the fog framework/network side to distinguish malevolent ambushes, for instance, port scanning, denial-of-service (DoS) etc. In fog computing, it bestows new prospects to explore how fog computing can offer with intrusion acknowledgment on both client some help with siding and the bound together cloud side. Authors of [Shi et al, 2015] have displayed a cloudlet mesh based security framework which cans recognizable proof interference to detachment cloud, sheltering communication among cloudlet, cloud and PDAs. There are in like manner troubles, for instance, realizing ID in generous scale, high-flexibility fog computing milieu to meet up the low idleness need.

4. CONCLUSION

Fog computing, a worldview that stretches out cloud computing and services to the edge of the network, meets improved prerequisites by finding information, calculation control or computation power, and systems administration capacities closer to end hubs. Fog computing is recognized by its openness to end clients, especially its backing for versatility. Fog nodes are geographically disseminated, and are employed near wireless access points in regions with a noteworthy use. Fog devices may take the type of stand-alone servers or system gadgets with on-board processing capacities. Services are facilitated at the system or network edge or even inside of end-client gadgets/tools, for example, set-top boxes or access points. This decreases services idleness/latency, enhances QoS and gives a better affair than the client. Fog computing holds up developing Internet of Things (IoT) applications that request ongoing or unsurprising inertness, for example, industrial automation, transportation, and systems of sensors and actuators. Because of the capacity to bolster a wide land dispersion, fog computing is all around situated for continuous or real-time huge information examination. Fog underpins thickly distributed data or information collecting points, adding a fourth hub to the regularly said Big data measurements 3V (volume, variety, and velocity). Issues of security and protection are in fog computing, however this remains understudied especially in the outline and execution of fog computing. Security elucidations exist for cloud computing, yet because of the hidden contrasts between cloud computing and fog computing, such arrangements may not suit fog computing gadgets/tools that are at the edges of systems/networks. In such situations, fog computing gadgets or devices face dangers that don't emerge in a very much oversaw cloud environment.

5. REFERENCES

[1] ”Dsouza et al ”, Policy-driven security management for fog computing: Preliminary framework and a case study, IRI. IEEE (2014)

[2] ”Dwork”, Di erential privacy, An Encyclopedia of Cryptography and Security. Springer (2011)

[3] ”Bonomi et al”, Fog computing and its role in the internet of things, workshop on Mobile cloud computing. ACM (2012) [4] ”Han et al”, A timing-based scheme for rogue ap detection, TPDS 22 (2011)

[4] ”Bouzefrane et al”, Cloudlets authentica-tion in nfc-based mobile computing, MobileCloud. IEEE (2014)

[5] ”Cash et al”, Dynamic searchable encryption in very-large databases: Data structures and implementation, NDSS. vol. 14 (2014)

[6] ”Damiani et al”, A reputation-based approach for choosing reliable resources in peer-to-peer networks, CCS. ACM (2002) [8] ”Balfanz et al”, Talking to strangers, Au-thentication in ad-hoc wireless networks, NDSS (2002)

[7] ”Dinh et al”, A survey of mobile cloud computing: architecture, applications, and approaches. WCMC 13 (2013)

[8] ”ETSI”, http://goo.gl/7NwTLE (2014) [11] ”Cao et al”, Privacy-preserving multi-keyword ranked search over encrypted cloud data. TPDS 25 (2014)

[9] ”Cao et al”, Lt codes-based secure and reliable cloud storage service. In: INFOCOM. IEEE (2012)

[10] ”Gao et al”, Location privacy in database-driven cognitive radio networks: Attacks and countermeasures, INFOCOM. IEEE (2013)

[11] ”Gil Press 2015”, http://goo.gl/zFujnE.

[12] ”Lu et al”,An efficient and privacy-preserving aggregation scheme for secure smart grid communications. TPDS 23 (2012) [16] ”Zhu et al”, Improving web sites performance using edge servers in fog computing architecture, SOSE. IEEE (2013)

[13] ”Zissis et al”, Addressing cloud computing security issues, Future Gener-ation computer systems 28 (2012)

[14] ”Han et al”, A measurement based rogue ap detection scheme, INFOCOM. IEEE (2009)

[15] ”J sang et al”, A survey of trust and reputation systems for online service provision, Decision support systems (DSS) 43 (2007) [20] ”McLaughlin et al”, Protecting consumer privacy from electric load monitoring, CCS. ACM (2011)

[16] ”Klaedtke et al”, Access control for sdn controllers, HotSDN. vol. 14 (2014)

[17] ”McKeown et al”, Open ow: enabling innovation in campus networks, ACM SIGCOMM CCR 38 (2008)

[18] ”Gennaro et al”, Non-interactive verifiable computing: Out-sourcing computation to untrusted workers, CRYPTO, Springer (2010) [24] ”Willis et al”, a multi-tenant platform for dynamically installed third party services on home gateways, SIGCOMM work-shop on Distributed cloud computing, ACM (2014)

[19] ”Yang et al”, Data storage auditing service in cloud computing, challenges, methods and opportunities, WWW 15 (2012) [26] ”Wang et al”, Privacy-preserving public auditing for data storage security in cloud computing, INFOCOM. IEEE (2010)

[20] ”Wei et al”, Flexible privacy-preserving location sharing in mobile online social networks, INFOCOM. IEEE (2012)

[21] ”Modi et al”, A survey of intrusion detection techniques in cloud., Journal of Network and Computer Applications 36 (2013) [29] ”Yap et al”, Separating authentication, access and accounting, A case study with openwi, open Networking Foundation, Tech. Rep (2011)

[22] ”Yu et al”, Achieving secure, scalable, and fine-grained data access control in cloud computing, INFOCOM. IEEE (2010)

[23] ”Parno et al”, Nearly practical verifiable computation, Security and Privacy, IEEE (2013) [32] ”Stojmenovic et al”, The fog computing paradigm, Scenarios and security issues, FedCSIS. IEEE (2014)

[24] ”Wang et al”, Enabling secure and e cient ranked keyword search over outsourced cloud data. TPDS 23 (2012)

[25] ”Ha et al”, Towards wearable cognitive assistance, Mobisys. ACM (2014)

[26] ”Valenzuela et al”, Real-time intrusion detection in power system operations, Power Systems, IEEE Transactions on 28 (2013)

[27] ”Zao et al”, Pervasive brain monitoring and data sharing based on multi-tier distributed computing and linked data technology, Frontiers in human neuroscience 8 (2014)

[28] ”Zhang et al”, Cloud computing: state-of-the-art and research challenges, Journal of internet services and applications 1 (2010) [38] ”Takabi et al”, Security and privacy challenges in cloud com-puting environments, IEEE Security and Privacy 8 (2010)

[29] ”Vaquero et al”, Finding your way in the fog, Towards a comprehensive definition of fog computing, ACM SIGCOMM CCR 44 (2014) [40] ”Qin et al”, Defending against unidenti able attacks in electric power grids, TPDS 24 (2013)

[30] ”Shin et al”, Network security monitoring using open flow in dynamic cloud networks. In: ICNP. IEEE (2012)

[31] ”Qin et al”, Preserving secondary users' privacy in cognitive radio networks, INFOCOM, 2014 Proceedings IEEE. IEEE (2014)

[32] ”Novak et al”, Near-pri: Private, proximity based location sharing, INFO-COM. IEEE (2014)

[33] ”Satyanarayanan et al”,The case for vm-based cloudlets in mobile computing, Pervasive Computing 8 (2009)

[34] ”Tsugawa et al”, Cloud computing security, What changes with software-defined networking?, Secure Cloud Computing. Springer (2014)

[35] ”Satyanarayanan et al”, An open ecosystem for mobile-cloud convergence, Communications Magazine 53 (2015) [47] ”Rial et al”, Privacy-preserving smart metering, Proceedings of the 10th annual ACM workshop on Privacy in the electronic society. ACM (2011)

[36] ”Song et al”, Practical techniques for searches on encrypted data, Security and Privacy, IEEE (2000)

[37] ”Shi et al”, Cloudlet mesh for securing mobile clouds from intrusions and network attacks, Mobile Cloud (2015)