Survey on Security Performance of Fog Computing and Existing Encryption Techniques

Sakshi Tripathi
Department of IT
Technocrat Institutes of Technology (Mains), RGPV, Bhopal,
Madhya Pradesh, India

Rakesh Kumar Tiwari
Department of CS
Technocrat Institutes of Technology (Excellence), RGPV, Bhopal,
Madhya Pradesh, India

Rajesh Nigam
Department of IT
Technocrat Institute of Technology (Mains), RGPV, Bhopal,
Madhya Pradesh, India

ABSTRACT

Fog computing is a standard partition infrastructure between edge and cloud computing. Fog computing and cloud computing are not the same they both have the features that make them different from each other but both have some uniform character because of this, here did not devote security and privacy assessment of cloud to fog computing like mobility, heterogeneity, etc. Fog computing is present as an intermediate layer work as an arm between cloud and edge computing. As the data increases, the security problems will be over. The essential problem in fog computing is its security because of finite resources. Cloud computing is technology here, any amount of data is stored online on a cloud server but cloud computing or servers of the cloud is miles from the end-user and this is the reason user faces a problem like lower latency so to deal with a problem a new technology called Fog computing is designed. In this survey, discussing the security concern of fog computing and will try to find the solution better than the existing solution as well.

Keywords

Cloud computing, Privacy issues, Security obstacle, Fog computing, Fog server, and Proxy server.

1. INTRODUCTION

The name fog computing refers to "edge computing". The content that something other than the running and hosting from the centralized cloud[1]. The system of fog conduct on network ends. It reduces the bandwidth needed by using a distributed layout. This outcome is lower cost and enhances efficiencies. Fog computing is one approach to hold the internet of things. Fog-computing can be called as edge computing/fogging, it is designed of responsibility application, data, and processing are stuffed in devices in the network edge. The terminology "Fog computing" was proposed by the cisco system. In fog computing equipment communicate to compeer just to efficiently share and store data and make native decisions**.** Fog computing implements processing at the edge network, while still contributing the probability to contact with cloud. The gigantic amount of data outgrowth from the connected application as well. Fog computing helps in road traffic clogging migration. Cloud computing is commonly a portrait for sanctioning acceptable, on-demanding network use of the mutual pool of configurable computing equipment (ex., server, application, storage, and network) that be immediately provisioned and liberated with least possible management or hawker interaction[2]. Cloud systems are placed within the internet, that is a trigonous network with the copious speed, technology, geologies, and types with no centric control. The other exceeding problem delay obstacle with cloud computing is security and privacy. Since cloud computing is based on the internet, data transmission, user requests, and system responses need to pass over a huge no. of an interposed network depends on the distance between the system and user[2]. The requirement of latency, delay jitter should be high in cloud computing. Geo distribution in cloud computing is centralized. The number of server nodes in the cloud is limited. Cloud computing is expected to facilitate computing directly to network at the edge, there is a fog computing or nodes that hand over new services and application for billions of connected equipment. As it is seen smart devices like smart meters, long scale wireless networks, and smart city/home connected vehicles face many types of problems like storage problems, bandwidth problems, computation problems, etc.

2. DIFFERENCE BETWEEN FOG COMPUTING & CLOUD COMPUTING

Cloud computing is a tremendous result if there is uninterested access to a cloud node that is able of transmitting data and processing the bulk of data speedily to the edge devices or end-user. The planning of fog computing mainly consists of heterogeneous devices, so in fog computing the management of services and kind of applications through smart devices at the node although the real management of the things is done by cloud-computing. Cloud computing, points the internet users while fog computing points generally mobile users. The type of services in cloud-computing is globalized whereas in fog-computing it is localized. Though the storage in cloud computing is higher than fog computing, it means fog computing has limited storage as compared to cloud storage. The connection between a user and fog computing is wireless because the distance is not far as compared to the cloud layer, But the communication between user and cloud is not so easy because of large distance, so through the IP network, it would be possible. Like fog computing, local security provided to cloud computing is tedious. If the comparison about parameters, Mobility in fog-computing is supported but in cloud computing, it is not supported. The number of service nodes in fog is more than a cloud[3].

Table 1. Fog computing Vs Cloud computing

FUNDAMENTAL	FOG COMPUTING	CLOUD COMPUTING
Target user	Mobile Users	Internet users

Location of server	Edge users	Within the internet
Servicing type	Localize information service	Global Information
Latency	Minor	Large
Delay jitter	Minor	Large
Number of server nodes	Large	Few
Response time	Sub-second	Minutes
Security	More secure	Less secure
N/W bandwidth	Low	More

3. FOG COMPUTING ANALYSIS

In the fog enforcement the movement takes place in a data hub or a piece of good equipment, or a good gateway or a router, they slow down the bulk of data sent to the cloud. all users get familiar with cloud computing more than that fog computing, it is a new approach. Fog computing is not the same they both have the features that make them different from each other but both have some uniform character and it is not easy to devote security and privacy assessment of cloud to fog computing like mobility, heterogeneity, etc. Fog computing is present as an intermediate layer work as an arm between cloud and edge computing. As the data increases, the security problems will be over. The major problem in fog computing is its security because of finite resources[3]. The terminology "Fog computing" was proposed by the cisco system. In fog computing equipment communicate to compeer just to efficiently share and store data and make native decisions. Fog computing implements dealing at the edge network, while still contributing the probability to contact with cloud. The gigantic amount of data outgrowth from the connected application as well. Fog computing helps in road traffic clogging migration.

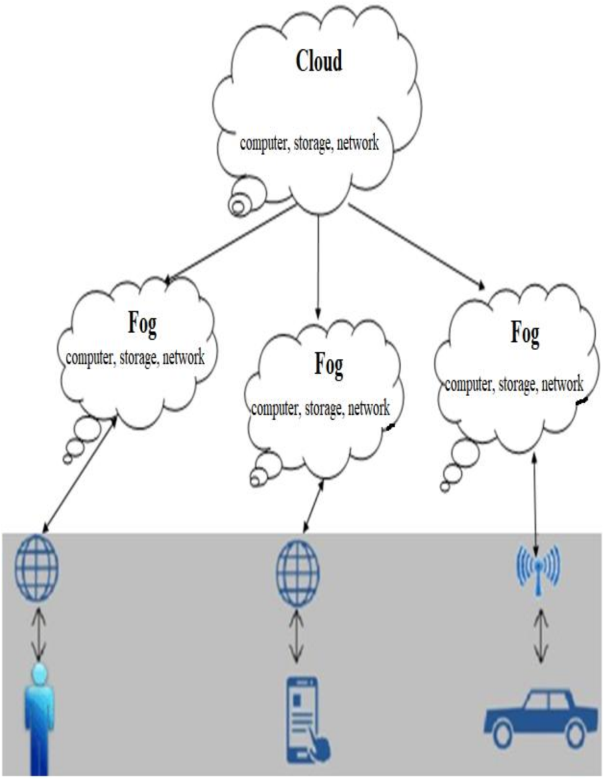
Cloud
computer, storage, network
Fog
computer, storage, network
Fog
computer, storage, network
Fog
computer, storage, network

Fig:1 Fog Computing Architecture

3.1 Fog Server and Proxy Server

In the hierarchy of fog computing, fog server is in the front end, Therefore security in fog computing needs a different standard for each application. Each application has its requirements as per standard and making security of this level is very difficult and complicated[3]. A Fog server is a similar work as a proxy server because the proxy server is a server that acts as an application-level gateway in the middle of a local network and large scale network. The proxy server serves security and heightened performance. In some of the cases, they handle employees that use outside resources. Like fog server act in between the cloud layer and edge layer, a proxy server acts as intercepting connections between the sender and receiver.

3.2 Fog Node

All devices that use computers to process information, entertain, manage, and communicate the things, having storage and associate connectivity are also called fog nodes. For example industrial controllers, routers, embedded servers, switches, and surveillance cameras[4]. Fog nodes are shared fog computing stuff enabling the categorization of fog services and assemble by fewest a single or more than single physical devices with sensing and processing capabilities (e.g, smart edge device, temperature sensor, mobile phone, computer, etc).

3.3 Fog Storage

Which is also called fogging or edge computing. All the operation related to data is done in storage. The operation of computers facilitates by fog computing. The operations in storage are also forward by the fog server, the services of networking between cloud server data centers and devices are also facilitated by fog computing.

3.4 Fog technology

The decentralized structure of fog computing of responsibility storage, data, and applications are occupying some space in the middle of the cloud and the data source[1]. Fog computing gathers the power and asset of the cloud imminent where information is acted and build upon

Table 2. Results issues or attacks with the existing solution found in fog computing

Attacks	Threats	Exist solutions
Communication medium	Hello-flood attack	Firewall
Middleware attacks	Sybil attack	Multipath routing
	Wormhole	TSL or SSL protocols
	Data disclosure	Packet authentication
	Selective forwarding	Link-layer encryption
	Blackhole attack	Password management
	Acknowledge flooding	IPSec protocol
	Heterogeneity	Auth broadcast
	Session account hijacking	Identity verification
	Insecure API and services	Encrypted communication
	Poor access control	Limiting the number of connection
Server attacks	Single jamming	Jamming report
On fog applications	Node capture	Cryptography
	Sybil attacks	Spread spectrum
	Spoofing attack	Authorization
	Node outage	Error-correcting
	Device tampering	Steganography
	Malicious data	Collision detection
	Node capture	Image processing
	Replay attack	Secure key management
	Illegal data access	Data masking
	Low attack tolerance	Network monitoring
Security issues	Sniffing attacks	Secure code
On web security,	Data loss	authentication
Wireless security	Cross-site request forgery	Secure routing
	Drive-by attacks	Periodic auditing
	Active impersonation	Firewall
	Data breach	Find and patch vulnerabilities
	Message distortion issues	Intrusion prevention system
	SQL injection	Private network
	Malicious redirection	
	Cross-site scripting	
Sensing layer	Information privacy	Data encryption
IoT attacks	Sniffer	Data verification
	Session hijacking	Session inspection
	Social engineering	Cache development
	Phishing attacks	Access control

	Node identification	Safe programming testing
	DDoS	Boundary inspection
	Injection	Safe programming testing
		Antivirus software's

4. SECURITY & PRIVACY OBSTACLE

Resources provided by the fog server to the end-user So, In fog computing, fog servers must check the reliability first to the end-user then resources should be provided securely. In this system the access of unauthorized persons is possible, this means none of the malicious users can access the fog services. These security attacks like insider issue attack, a man in the middle attack, session key recovery, gateway compromise, impersonation attacks, reply attacks, password guessing attacks, and one of the important attacks are mutual authentication. On the other side, security obstacle is also considerable between the cloud and fog computing if some kind of consequential data is transmitted. Such attack, impersonation attack, man-in-the-middle attacks, man-in-the end attacks, and the very important thing is searching issues, protect file storage, and at the end of the cloud-fog server the key management issues.

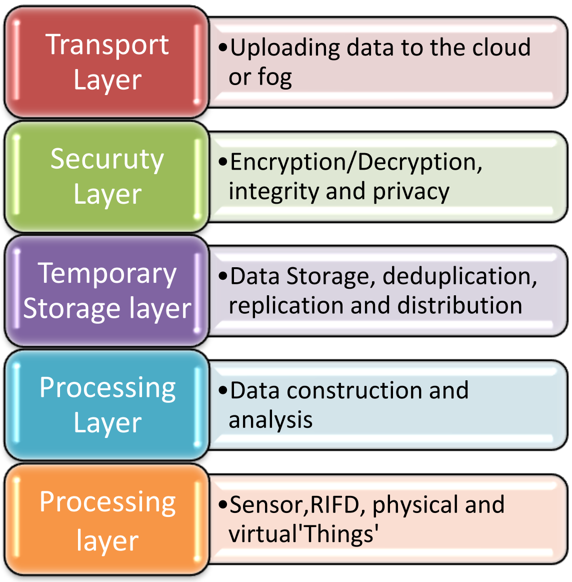
Transport Layer
•Uploading data to the cloud or fog
Securty Layer
•Encryption/Decryption, integrity and privacy
Temporary Storage layer
•Data Storage, deduplication, replication and distribution
Processing Layer
•Data construction and analysis
Processing layer
•Sensor,RIFD, physical and virtual'Things'

Fig:2 Fog Layers

4.1 Authentication

Secure communication between the end-user is also a risk factor in the cloud fog computing model. Sometimes unauthorized creates several security threats and launch it over the server. It needs a robust authentication protocol that would be challenging to establish in the cloud-fog-computing model. Here is discussing security threats in this section, Attackers can hack the system by throwing threats[5]. For some users maintaining high entropy, the password is a very tough job, they either use a common dictionary word or they use their details like birth date or name and it is easy for a hacker to guess the password by cryptography method[6]. So, password protection plays an important role to secure the data so that threats shall not break the security system and can keep important data safe in the first place.

4.2 Privacy

Privacy is related to personal data or information that should not disclose by others except those, users choose to share. It is considered a very important feature in fog computing. With the development of the digital age, private data vulnerabilities have enhanced[7]. The thing which gains attention in the privacy field of networking is the leakage of personal data. The fog server holds a piece of very sensitive information and because of this end-user access fog node more than the cloud nodes. To finish this issue an encryption method called home area network(HAN) is used.

Privacy is applied in so many ways along with data masking, encryption, and authentication. each effort is to ensure that the data is available only to those users if they are authorized, persons.

4.2.1 Location Privacy

Privacy refers to the location of the client in fog is known as location privacy. In privacy, location privacy is an important security aspect. The control in individual access to his or her current location and past location information is the capability of location privacy[8]. The shortage of location privacy maybe leads to consequent disclosure of knowing traffic information on the network and physical world. The location privacy is in danger as long as a fog client is connected with user information and important object.

4.2.2 Usage Privacy

Before it has known the privacy issue in data usage privacy, it is essential to know about data usage. All users are using mobile data if mobile phones are not connected with wifi. Data usage is generally a bulk of data that is used in the billing cycle. Usage pattern that used by fog clients in fog service is another privacy issue. For instance smart grid, its meter reader detects the household information such as at what time TV is turned on, or if any person present in the home is already breaching user privacy, however, to preserve the privacy mechanism has been proposed in the smart meter[9]. But due to poverty of trusted third party (Smart meter or a device like a battery), it cannot be applied directly in fog-computing because nodes in fog can statics the usage of end users one possible way is to create dummy task and offload it to those nodes and hide the real task will be hidden among the dummy task. Although it will escalation the client payment and wastage of energy and resource, there is another smart solution in which the application is partitioned to monitor the usage of private data.

4.2.3 Data Privacy

Data privacy is also called as information privacy. Data privacy is simple to understand, it just makes your data private. Data can be personal data or recorded data like criminal records, medical records, business-related data, political data, and website information they all need to maintain and privacy-preserving. Privacy is applied in so many ways along with data masking, encryption, and authentication. Each effort is to ensure that the data is available only to those users if they are authorized, persons.

4.3 Network Security

One of the issues is related to network, a fog node generally connected with the huge number of small devices[10]. Some devices generate a small amount of data and some devices generate bit large data but the data of all devices have combined the bulk of information becomes difficult to handle. Hence, connected with heterogeneous mechanisms, managing the network, fog nodes, connection in the middle of each device will be a concern unless NFV and SDN techniques are applied[11]. The world is full of the network. It needs more security to secure data over the network.

4.4 Secure Data Storage

If there is huge data, then it needs storage servers, the cloud is also used to store these bulk data that can be achieved easily. But the main concern is the security of the data, that should not be accessed by unauthorized and research for securing the data is still going on for frequently used data[12]. Cloud Fog also used in the cloud server. Cloud is also used to store bulk data and storing the data can be easily achieved. The database for data storage is possible in both fog and cloud servers. But the main challenge is to secure the fog data as data can be easily accessed by unauthorized by using high standard techniques. Data is stored in the fog without high-level security and it may possible that it can be hacked easily. Several types of research have been done to implement security by encrypting the data. The key has to be maintained for encrypting and decrypting the data, similar to a fog cloud is also facing this issue[13]. Securing the data is still not fully implemented and hence optimized algorithm is required to achieve an end to end security. Cloud is also used to store bulk data and storing the data can be easily achieved.

4.5 Data Integrity

In this concept, the message sent by the sender is the same as the receiver receives[14]. This one is the important feature required in fog and cloud computing infrastructure. If the user, in the end, wants to access information from the cloud server or fog server, it should be compulsory to serve data integrity. The hash function is one of the existing solutions to cryptography[15]. Many algorithms are applied to provide strong integrity like SHA-1, MD5, SHA-2, etc. Many researchers have been work for a long time just to get strong property of data integrity but still, it is a challenge of open research for fog and cloud computing[16].

4.6 Intrusion Detection

IDS(Intrusion detection system) is equally very important just like other security attacks in the cloud-computing server. To serve safeguard on denial-of-service assault, insider attack, flooding attacks, and port scanning attack .malicious user send inapplicable information to the receiver and build an excess of data to the receiver to conduct DDoS or DoS(denial of service) attack at the same time of communication[1], because of this it is necessary to locate Intrusion detection system method in the fog devices to analyzing information of user-related, control access policies, logs file, etc and monitor the intrusive behavior. Many existing Intrusion detection system algorithms are available but discuss the performance it is not enough in terms of security. IDS is still a security challenge for the researcher to design a better and new algorithm and it should be efficient for IDS. The same concept is required for IPS (Intrusion prevention function) at the cloud and fog server as well.

5. APPLICATION AREA

Table 3 Security problems present in the application

Applications	DOS	DB	DL	IA	API	MI
Energy Reduction		✓	✓			
Smart Meters			✓			✓
Vehicular Network	✓	✓				
Augmented Brain Computer		✓			✓	
Speech Daa			✓			

DoS: Denial of service, DB: data beeches, DL: data loss, IA: Insecure APIs, API: advance persistent threats, MI: malicious insider.

5.1 Energy Reduction

A new thing which can be done through fog platform is the reduction of energy. Reduction of energy is based on numbers of downloads, information pre-loading, the amount of idle time, and updates. As it seems that a large amount of energy is required in cloud operations, different types of applications required different energy[17]. A server called Raspberry Pi server of responsibility applications has investigated is configured and installed in a fog platform to slow down energy consumption. Some applications produce continuously static data in a period of end-user limits and have a lower rate of connection(ex., surveillance, video), that can easily save the efficient amount of energy through the fog.

5.2 Smart Meter

Fog computing helps in the improvement of the bandwidth capacity of the hardware. The process of data aggregation takes along time to process because of low bandwidth capacity after developing a smart grid, a bulk of data is recorded, process, and transmit from smart meters by using DAU(data aggregation unit). The data is generated in meter storage from there the MDMS(meter data management system) uses that data for forecast energy demands in the future. The thing that is done in this application is fog devices like the router that is connected through smart meters. To make this application better.

5.3 Vehicular Network

A new fog based application is develop known as vehicular network. The architecture is proposed by fog computing in the manner for road safety. The complete name of this network is VANET(Vehicular Adhoc Network). This system has threelayer architecture: upper, middle, and lower. The upper layer help in deciding traffic violation and alert related authorities. In the middle one layer, fog server assures that if a person drives a vehicle, purposely offend the rules and communicate transport identifier data to the cloud server[16]. In the last layer called lower layer is capable to know out handheld devices while driving and detect transport number using camera sensors and transmit the data to nearby fog server.

5.4 Augmented Brain Computer

A multi-tier infrastructure fog computing develops a new technology called a brain detention system, Hence it can detect the mental state of real-time[18]. Fog server separates characters like time frequency from sign and consigns them to the classifiers of mental state. The advantage of this application is to demonstrate playing online multi-player games known as tractor beam EEG. Augmented brain-computer, a wearable system that is used to determine the real state of a human's mind. This device will provide a direct connection between the brain/nervous system of the human and electronic devices. As it is known that 5G will provide very high speed, high bandwidth, low latency, etc And can say that 5G will be helpful in the implementation of augmented brain-computer because these factors are very essential for the implementation. In the augmented brain-computer system, 5G reduces data congestion, provides high data transfer, provides the frequency of the high band. At least can speak now the 5G will make the Augmented brain-computer system a faster device.

5.5 Speech Data

An interface called FCI (fog computing interface) is newly developed for smart things or new trend devices like smart android watches that connected through the smart tablet, that collects data, records data, and processing on speech data of Parkinson's disease from patients[19]. Fog computing interface takes out some important information from collected data, instead of addressing complete data like short-time energy, spectral centric, volume, and zero-crossing rate from speech data and for long term analysis, it is sent to the cloud. six patients were tested by this application and fog computing made it possible. In a less time fog computing, remotely process huge amount of speech/audio data.

5.6 5G Mobile Network

5G is the Fastest wireless communication and highly supported by WWWW (wireless world wide web). It has 100 times better internet capacity than 4G. With 5G traffic can handle 1000 times better than today[20]. Foundations of 5G are as follows Small cell, Millimeter waves, Massive MIMO (multiple-input and multiple outputs), Beamforming, and Full Duple. Suppose, a person wants to watch/install movies then 4G will take 50 milliseconds whereas for the same 5G will take 1 millisecond. But as its known frequency is very high, the signal didn't cross the obstacles like buildings, trees, heavy rainfall, etc.

6. CONCLUSION

In this paper, here discuss severable security obstacles related to cloud and fog server as well as computing. Fog computing is a new promising computing fundamental. Discussion about the comparison of fog and cloud computing. That tells us that the performance of fog computing is much better as compared to the cloud, but both the computing faces a similar type of security problem. Enhancing the security of cloud computing environments is necessary nowadays to save the data from unauthorized access. Also focus on security and privacy obstacles like privacy in location, information privacy, and data usage privacy, in fog computing the determination of this survey is to enlarge the security level of fog-computing. Develop the open planning, and examine it via fog computing use study or view and testbeds, is the job of the open fog union. Fog computing design is strong for network separation and modifies energy and modifies frequency. To work with fog, must enable rapid, secure transmission, and trusted. Remote energy extraction and exploration, drone_enable supply chain, smart traffic, virtual reality, emergency response, and smart cities are just an example of appearing use study that is facilitated and enhanced through the fog. Fog computing drives the bandwidth, computing, and energy essential for opportunity explication and timely risk in the geographically challenged, data_intensive process and disruption-prone. Better than assemble data in the cloud to deal with, fog equipment from decoy network to flood data handling task and convey with each other to figure out the sub-serves image in the network. Fog architecture is a fundamental framework to test and build a new concept.

7. REFERENCES

[1] Kunal S, Saha A, Amin R. An overview of cloud-fog computing: Architectures, Applications with security challenges. Security and Privacy. 2019;2:e72.

[2] Akhilesh Vishwanath, Ramya Peruri, Jing (Selena) He," Security in fog computing through Encryption", International Journal of Information Technology and Computer Science(IJITCS), Vol.8, No.5, pp.28-36, 2016 DOI: 10.5815/ijitcs.2016.05.03

[3] Deepak Puthal, Fog computing security challenges, and future directions, ResearchGate, May 2019.

[4] Abebe Abeshu Diro, Naveen Chilamkurti, Yunyoung Nam. Analysis of Lightweight Encryption Scheme for-to-things Communication. Asan 31638, South Korea. IEEE,2018.

[5] Ionita M-G, Patriciu V-V. S secure threat information exchange across the internet of things for cyber defense in a fog computing environment. Inf Econ. 2016;20(3): 16-27.

[6] A. Dior, N. Chilamkurti, and N, Kumar, "Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog-computing", Mobile Netw. Appl., vol. 22, no. 5, pp.848-858, 2017.

[7] Yung Guan, Jun Shao, Gui Yi Wei, Mande Xie, Data Security, and privacy in fog computing IEEE.

[8] Yang R, Xu Q, Au MH, Yu Z, Wang H, Zhou L. Position-based cryptography with location privacy: a step for fog computing. Futur Gener Comput Syst. 2018; 78:799-806.

[9] I. Stojmenovic, "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," in Proc. IEEE Austral. Telecom. Netw. Appl. Conf. (ATNAC), Nov. 2014, pp. 117-122.

[10] Shikha Mathur, Vishal Goar, Deepika Gupta, Manoj Kuri, Analysis and design of enhanced RSA algorithm to improve security, IEEE 3rd International conference on "Computational Intelligence and communication technology" IEEE-CICT 2017

[11] A. A. Dior, H. T. Reda. And N. Chilamkurti, "Differential flow space allocation scheme in SDN based

fog computing for IoT applications," j. Ambient Intell. Humanized Comput., pp. 1-11, Jan. 2018.

[12] C. Dsouza, G. J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: preliminary framework and a case study," in Proc. IEEE 15th Int. Conf. Int. Reuse Integer. (IEEE IRI), Aug. 2014, pp. 16-23

[13] M. Green and G. Ateniese, "Identity-based proxy re-encryption", in Applied Cryptography and Network security. Berlin, Germany: Springer, 2007.

[14] Mohammed, E.M, Ambelkadar, H.s, "Enhanced Data Security Model on Cloud Computing", International Conferences on IEEE publication 2012, on pages(s): cc-12-cc-17.

[15] D. Hankerson. S. Vanstone, and A. J. Menezes, Guide to Elliptic Curve Cryptography. New York. NY, USA: Springer-Verlag, 2004.

[16] Neha Shrikant Dhande, FOG COMPUTING: REVIEW OF PRIVACY AND SECURITY ISSUES, International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015

[17] Naranjo PGV et al. P-SEP: a prolonged stable election routing algorithm for energy-limited heterogeneous fog-supported wireless sensor networks J Supercomput. 2017;73(2):733-755.

[18] Peter N. Fog computing and its real-time applications. Int J Emerg Technol Adv Eng. 2015;5(6):266-269.

[19] Monteiro, Admir, et al. "Fit: a fog computing device for speech data-treatments." 2016 IEEE International Conference on Smart Computing (SMARTCOMP). St. Louis, MO: IEEE, 2016.

[20] Chiang, Mung, and Tao Zhang. "Fog and IoT: an overview of research opportunities." IEEE Internet Things J 3 (6) (2016): 854-864.