ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

A Survey on Fog Computing and Its Security

Neethumol Kumar [1], Anandhu Pavithran [2]

M.Tech Student, School of Computer Sciences, Mahatma Gandhi University, Kottayam, India[1]

NeST, Aluva, India[2]

ABSTRACT: Fog computing is a new concept that broaden the cloud services by providing computing resources on the edge of a network and facilitate services similar as cloud such as networking, computing, storage, control and communication. In addition, fog concept is able to analyse large amount of data consequently, it's highly portable to IoT (Internet of Things) But, the fog computing era additionally rise up the hazard to privacy and security of the information and services. In this paper, we survey about a top level view of the present current issues and challenges in fog computing.

KEYWORDS: Fog Computing, Cloud, IoT, Security

I. INTRODUCTION

In today's world, whether it's small or large enterprise, the way to store and access information has taken a massive revolution is called Cloud Computing. Transferring and carrying the data on a physical device has become outmoded now. Fast growing technologies makes user friendly concept and the user can open the door at any time in the world. The major impartial of cloud is to apply approach in different areas like healthcare, transportation smart mall and smart homes. To achieve these cloud computing utilize shared pools of networks system and servers. At the earliest, they observe how would connect everything in the world to the cloud at cost effective way. At the time they realize and describe a new approach is IoT (Internet of Things).

Smart objects or things (hospital equipments, home appliance, vehicles and devices) are connected to the internet is defined as IoT. The smart thing's which are connected and possess using one or more sensors. Each sensor will connect to each other and collect, monitor and record the condition about location, image, temperature, motion, pressure, chemicals, gas etc. There is a growing comprehension this tendency will purse as growing numbers even simpler (home appliance) or highly constrained devices (medical equipment) get connected to internet [1]. Many of these applications work in real scenario, processing and computing in an accurate time. In order, to address the ever-increasing demand for computing and processing information, Cloud computing is the major and widely adopted commodity, conceptually supported by its massive storage and huge processing capabilities to work in real scenario. Nevertheless, cloud has met some restriction of IoT. The particular distinct of IoT need strict low latency. This is turn, has led to further innovations in the area of Cloud computing under the umbrella of Fog Computing concept.

Fog computing concept is a demoralization computing architecture whereby data is processed, analyzed and stored between the source and a cloud. These consequences in the cute rate of data communication overheads, and afterwards, improves the consummation of cloud by reducing the requirement to process and store large volumes of redundant data.

The Fog computing concept is mainly motivated by a continual grows in Internet of Things (IoT) devices, where an ever rise amount of data (with respect to volume, variety, and velocity) are produced from an ever-growing array of devices. IoT devices provide rich functionality, such as connectivity, and the development of new functionality is often data motivated. These devices need computing resources to process the acquired data; however, fast decision processes are also required to maintain a high-level of functionality. This can present scalability and reliability issues when utilising a standard client-server architecture, where data is sensed by the client and processed by the server. If a server

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

was to become overloaded in traditional client-server architecture, then many devices could be rendered unusable. The Fog paradigm aims to provide a scalable decentralised solution for this issue. This platform is capable of filtering, aggregating, processing, examine and transmitting data, and will result in saving time and communication.

Many researchers and commercial infrastructure developers believe that Fog platforms will be developed and released in the future to provide an enriched and more reliable infrastructure to handle the ever increasing expansion of connected computational devices. However, secure communications are among the issues that raise the most concerns from users when they use fog computing to transmit their data to the cloud to be stored and processed. In general, the significant threats in fog computing networks are:

***A. Data Alteration*:** An enemy can bargain records uprightness by method for endeavoring to alter or harm the legitimate actualities. Thus, it is essential to characterize a security component to offer records trustworthiness confirmation of the transmitted realities between the fog and the cloud.

B. Unauthorized get entry to: an adversary can attain accesses to unauthorized facts without permission that could result in loss or theft of data. This assault raises a safety problem that could reveal a user's personal facts.

***C. Eavesdropping Attacks*:** eavesdroppers can benefit unauthorized interception to research loads about the consumer data transmitted through wireless communications. The chance of such assaults is they can't be effortlessly detected because eavesdropping does no longer alternate something in the community operations.

This survey is structured as follows. Section II presents the Fog computing overview In Section III, we analyze security in Fog computing and architecture. Section IV presents the existing fog security mechanism. In Section V, we present the discussion and analysis. This survey is concluded in Section VI.

II. RELATED WORK

In this section, we briefly give an overview of fog computing and related work.

Fog computing is a concept with limited capability such as computing, storing and networking offerings in dispensed manner among extraordinary devices and classic cloud computing. It provides a splendid for IoT applications which can be latency-sensitive. Even though the time period turned into at first coined through Cisco [2], fog computing has been defined by using many researchers and businesses from some of exceptional views. [3] Have supplied a well known definition of fog computing. It is stated as; "fog computing is a geographically allotted computing architecture with a aid pool which consists of one or more ubiquitously related heterogeneous devices (which include aspect devices) at the brink of network and no longer completely seamlessly subsidized by using cloud services, to collaboratively offer elastic computation, garage and conversation (and many other new offerings and duties) in remote environments to a huge scale of clients in proximity". While, Vaquero and relate fog computing as; "a scenario in which a big range of heterogeneous (wi-fi and on occasion self reliant) ubiquitous and decentralized gadgets communicate and potentially cooperate amongst them and with the network to perform garage and processing responsibilities without the intervention of unauthorized parties. Those responsibilities may be for helping basic network capabilities or new offerings and programs that run in sandboxed surroundings. End users sublet chunk of their devices to hold those facilities get stimulus for implementing so". Fog computing is likewise described by way of the open fog consortium [4] as; "a machine-level horizontal structure that distributes assets and offerings of computing, storage, manipulate and networking anywhere from cloud to things". Table 1 summarizes Fog definitions provided by various research works.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

REVIEWED JOURNAL	CONTRIBUTION
Cisco[2]	Extends the Cloud Mainly used for IoT Can be establish anywhere Fog device consists of processing, storage, and network
Vaquero and Rodero-Merino[3]	heterogeneous, ubiquitous and decentralised devices communication Storage and processing done without third party invention Run in a sandboxed environment Leasing a part of customers gadgets and Offer incentive
Bonomi et al.[5]	greatly virtualized occupy between IoT devices and cloud Not exclusively located at the edge

Table 1: List of Reviewed Journal

We analyzed the search occurrence of fog and different related technology in Google scholar. Similarly, the range of papers to be had in one of a kind virtual libraries related to the fog became additionally analyzed. [6] Google scholar search occurrences of various comparable technology to fog were investigated in the beyond few years, as shown in Figure 1. According to the facts, edge computing is the topmost searched object in Google as compared to different comparable technologies. However, the hunt trend decreased by means of greater than three times inside the past 8 years edge computing. Mobile cloud computing and Mobile Edge computing are the opposite two pinnacle-searched computing paradigms after edge computing. The lowest trend located turned into for dew computing and fog dew computing. Whilst the trend for aspect computing is decreasing, Fog computing associated with scholarly searches is growing year by way of year, and has extended by means of 2.5 instances from 2010 to 2017. This suggests that fog computing is the quickest developing research place in academia and could have an incredible effect on the industry as well.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

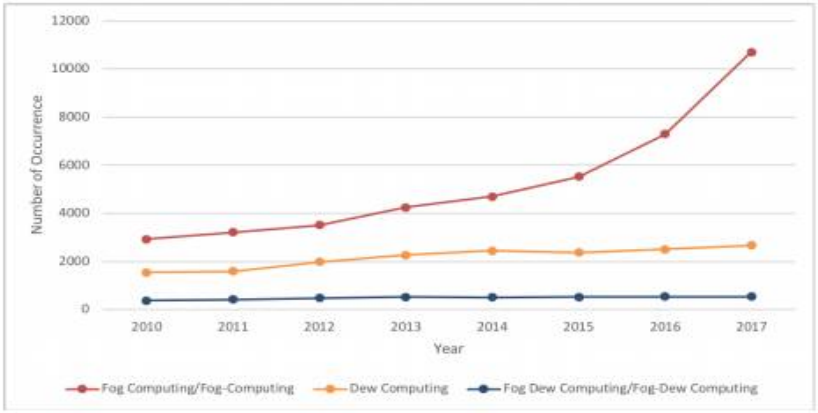

Figure 1: Search occurrence of Fog in Google Scholar

Three Tier Architecture of Fog

For marketplace adoption and deployment, fog computing need to. Have a widespread structure. There can be no to be had famous architecture so far. But, many studies works have presented fog computing architectures. In this segment, we first off talk the three tier structure of fog computing [6] shown in Figure 2.The three tiers are clarified beneath,

Tier1- IoT devices: This tier embrace of IoT devices which include smart devices such as smart phones, smart home, smart health equipments, smart cities and others.

Tier2- Fog: This tier is specified as fog computing situated between cloud and IoT. The fog nodes consist of router, gateway, and switch. These fog nodes helps to control, storage, communication and computing facilities.

Tier3- Cloud: This tier consists of cloud it provides shared pools of services such as control, storage communication and computing.
In Fog, data generated by Tier-1 devices (sensors, smart devices) will transmit to the middle Tier-2 is known as Fog which placed close to data source (Tier-1).These Tier-2 are capable of handling the operation with less computation power and less storage. Therefore, Tier-2 no needs to transmit data to Tier-3 for processing. Since, Tier-2 can able to process the data more efficiently and provide responses quicker than Tier-3. In fact, Tier-2 must meet all security criteria otherwise possibility to attack the intruder.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

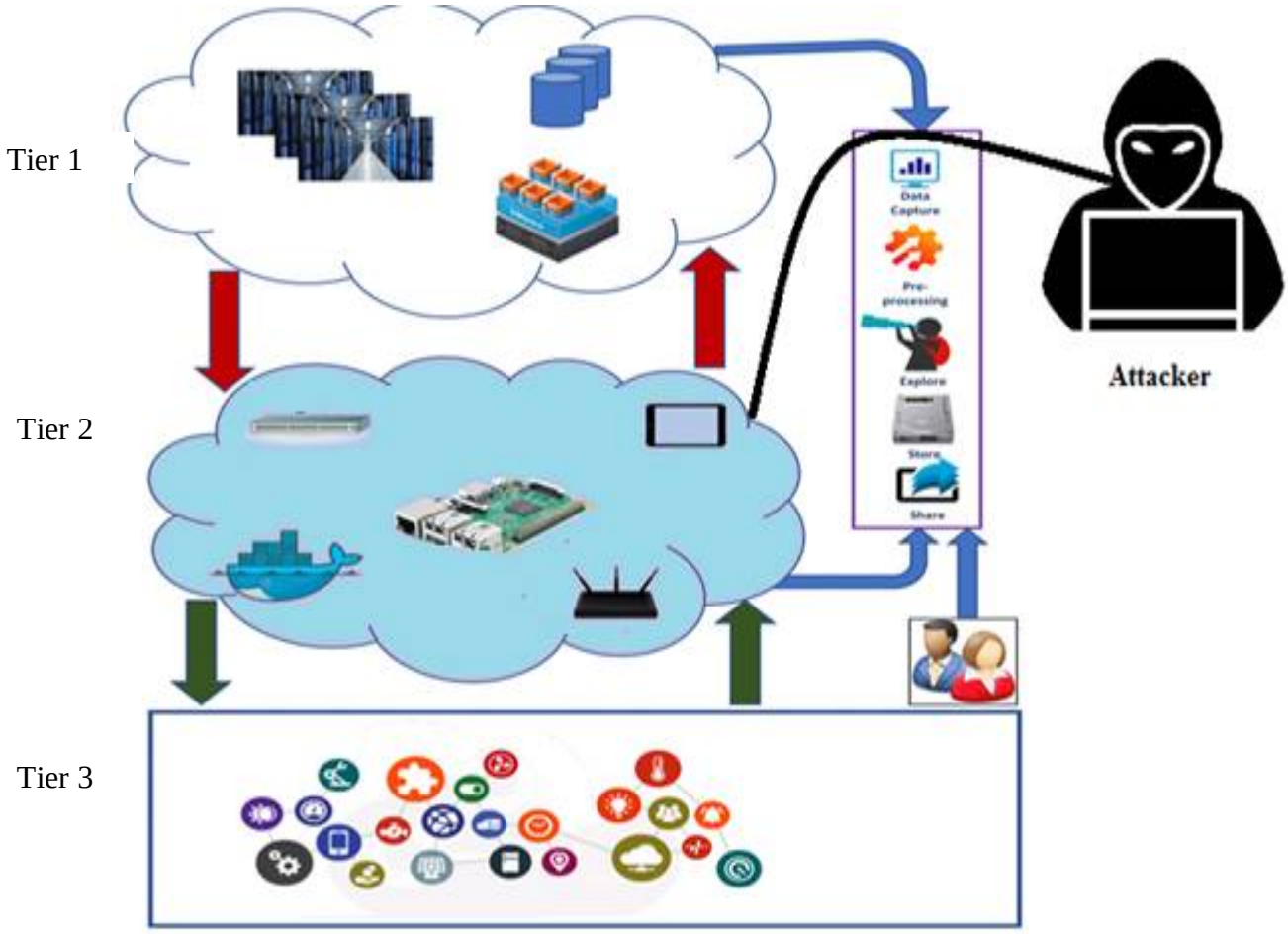

Figure 2: Three Tier Architecture of Fog

III. SECURITY IN FOG COMPUTING

The Fog concept demand also is flexible regarding attacks, trustworthy, data security and privacy. In this chapter we focus on various criteria for a security algorithm in fog.

On the grounds that fog is deemed as a non-trivial extension of cloud, some security and privacy problems within the context of cloud computing [7], may be foreseen to necessarily impact fog computing. Protection and privacy issues will lag the promotion of fog computing if now not well addressed, in line with the reality that 74% of it. Executives and leader statistics officials reject cloud in time period of the dangers in security and privateness. As fog computing is still in its little one level, there may be little works on safety and privateness troubles. Considering fog computing is proposed in the context of net of factors (IoT), and originated from cloud computing, Security and privateness issues of cloud are inherited in fog computing. On the same time as a few issues may be addressed using existing schemes, there are different issues going via new demanding situations, due to the awesome developments of fog computing, collectively with heterogeneity in fog node and fog network, requirement of mobility useful resource, large scale geo-distributed nodes, location-awareness and low latency. Due to these features of fog computing, we may need future work to tackle those security problems.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

A. The Criteria of an Ideal Encryption Algorithm in Fog

Confidentiality: Everyone has their own information they wish to keep as confidential, so that the encryption algorithm must satisfy confidentiality (protecting the collected data from unauthorized parties or competitor). Moreover, it can make sure to prevent eavesdropping and data leakage. In Fog computing a huge volume of data get produce from IoT devices since, security algorithm must provide highest levels of confidentiality.

Scalability*:* Encryption algorithm must satisfy scalability because multiple users need to load, store and transfer data via fog. The encryption algorithm must have capacity to handle multiple users at a time without affecting the performance.

Integrity: The data integration is a most important feature for Fog computing concept. The objective of Fog is to avoid alters or tampered data by the competitor that may give the wrong feedback from user. Secure data integrity mechanisms must be needed in encryption algorithm to attend users trust.

Availability: Refers to ensuring the authorized users are able to access the data when needed anywhere at any time. Algorithm must provide authorized user can access it at any time without delay.

B. Existing Fog Security Mechanism

In this section, we review the existing fog security mechanism shown in Figure 3.

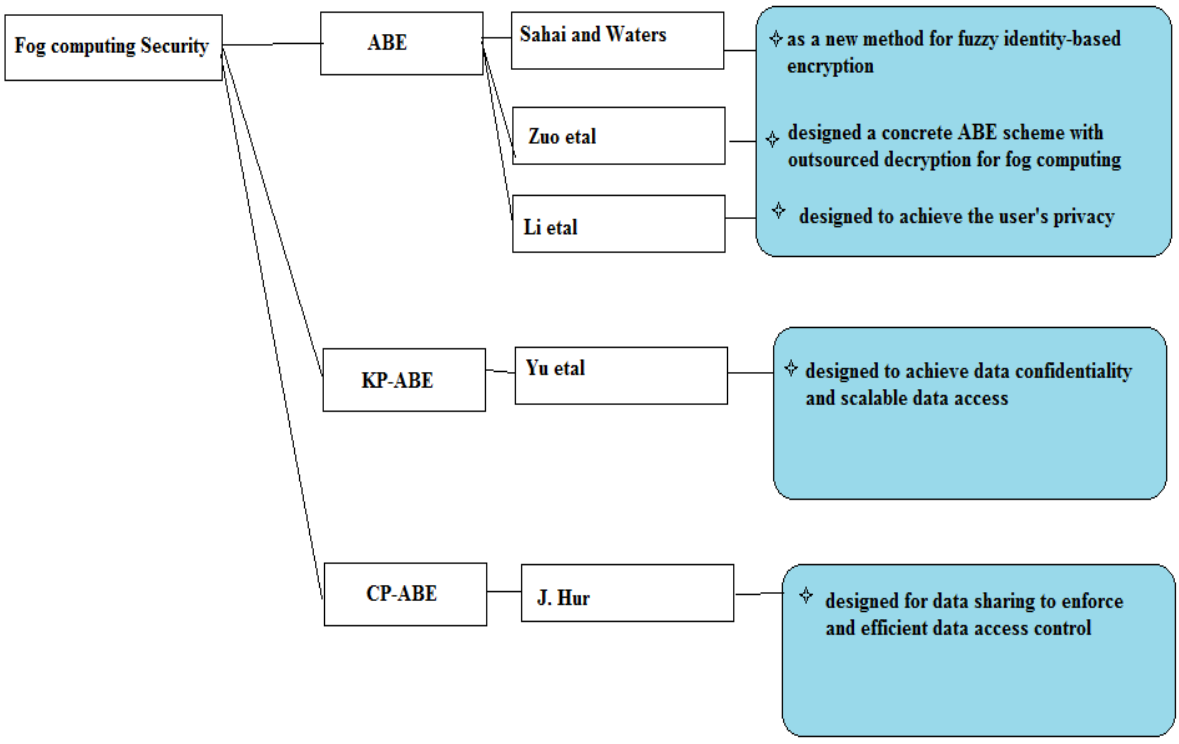

Figure 3: Existing Fog Security Mechanism

C. Attribute Based Encryption (ABE)

The thought of ABE was first presented by Sahai and Waters [8] as another technique for fuzzy identity-based encryption. They used the ABE scheme to achieve user's privacy and data access control. Authorize users in this scheme, and the keys are generated by using sender attributes and these attributes contain public key and private key. If the sender or the receiver needs to encrypt or decrypt the data, they can use this public or private key. To encrypt the data, use users attribute and create public and private key for decryption. For decrypting this data, match the key with the private or public key of sender attribute shown in Figure 4.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

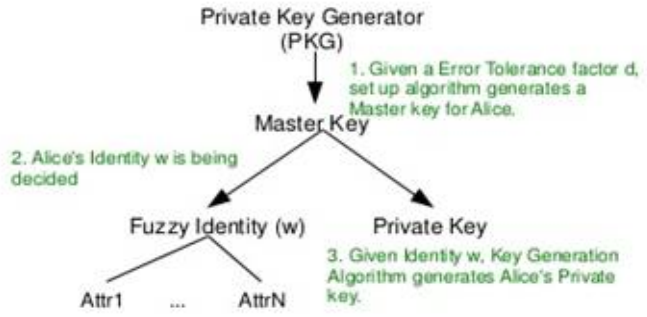

Figure 4: Workflow of ABE

Zuo et al. [9] they designed a concrete ABE scheme with outsourced decryption for fog computing.
Li et al. [10] proposed a patient-centric structure for information sharing access control to individual wellbeing record put away in cloud servers. They utilized the ABE strategies to accomplish a high level of the client's protection and a fine-grained information get to control for individual wellbeing records.

D. Key Policy Attribute Based Encryption (KP-ABE)

It is a modified scheme of ABE. Key Policy Attribute Based Encryption scheme is depict for one to-many communication in fog. In KP-ABE scheme, the key generated by using user attributes that creates a master key for encryption. If receiver decrypt the data using sender master key and public key, encryption is possible only if the attribute and master key match the user key (key policy) shown in Figure 5. The KP-ABE scheme can achieve secure communication between one to-many fog nodes and more flexible to handle users than ABE.

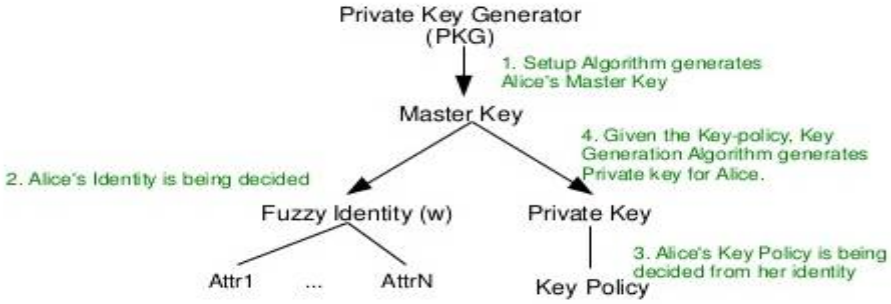

Figure 5: Workflow of KP-ABE

Yu et al. [11] combined KP-ABE with other methods to achieve confidentiality and scalable data access in the cloud server.

E. Ciphertext Policy Attribute Based Encryption (CP-ABE)

CP-ABE is the remodel form of KP-ABE and works in the reverse way. In a CP-ABE scheme, private key is established from the set of attributers of users and a ciphertext stipulates a policy over a describe universe set of

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

attributes. A receiver may able to decrypt in the case that user attribute satisfy the access policy of the appropriate ciphertext shown in the Figure 6.

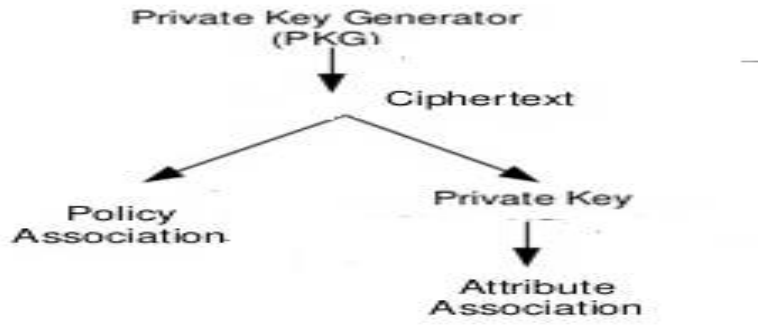

Figure 6: Workflow of CP-ABE

Hur [12] proposed a new CP-ABE scheme for information-exchanging to implement an efficient data access control based on the information sharing characteristics.

IV. DISCUSSION AND ANALYSIS

The criteria contain confidentiality, scalability, Integrity, availability. The comparison table is listed in Table 1.

Scheme	Confidentiality	Scalability	Integrity	Availability
ABE	Yes	No	No	No
KP-ABE	Yes	No	Yes	Yes
CP-ABE	Yes	Yes	Yes	Yes

Table 1: The criteria of an ideal attribute-based encryption scheme

The ABE scheme only satisfies confidentiality. Because the private key based on user attribute, using that key we can decrypt the data. The scheme only achieves the basic security confidentiality. In KP-ABE scheme, they cannot achieve scalability but all other requirement meets this encryption scheme. CP-ABE scheme [11] satisfies all the basic security requirements.

F. Security Analysis of Algorithm Using Some Attacks

We analyse the security criteria with the aid of a few primary attacks.

Denial of Service: Dos attacks can deliver down the rendering services of fog network by aiming to attack protocols of community or by shelling the fog community with excessive site visitors. DoS attack is understood to be the most commonly used assault which signifies a category of assault that might bring about fog.

Man in the Middle Attack: the character inside the middle attack intercepts a malicious node amongst communicating nodes which may be managed with the aid of adversary in fog. The malicious device can act as a middle device by eavesdropping a few of the nodes and identity statistics of the two regular gadgets whilst start communicating to save and beforehand all statistics. Even as two nodes can't stumble on the eavesdropper, as an alternative they expect that they will be talking directly.

Brute Force Attack: A brute force attack is an ordeal-and-errors approach used to acquire facts inclusive of a person password or private identification quantity (PIN). In this attack, computerized software is used to generate a massive quantity of consecutive guesses as to the important of the favored records.This attacks can be utilized by culprit to crack encrypted statistics. A brute force attack is also called brute force cracking.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

Dictionary Attack: A dictionary assault is primarily establish on trying all of the strings in a pre-organized listing, commonly derived from a listing of phrases such as in a dictionary (as a result the word dictionary assault. We analyse these attacks in various security scheme shown in Figure 7.

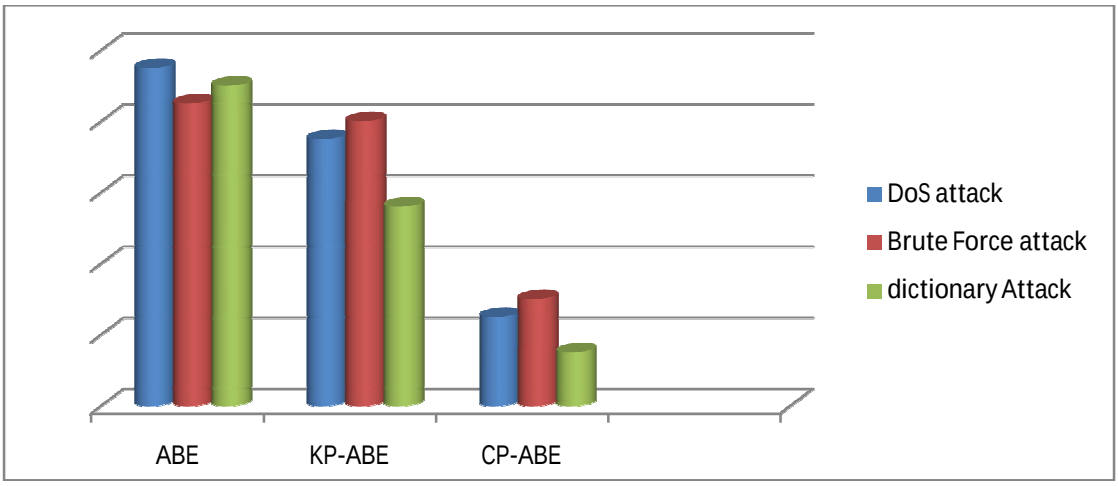

Figure 7: Attacks in Various Security Scheme

The above chart shows the possible attack in fog computing. There are three colours on the chart. The DoS attack is represented by the blue color. The brown colour represents brute force attack. The gray colour represents dictionary attack. The chart demonstrates that, various attack possibility in Fog security scheme. In ABE scheme, higher possibility to attack compared with KP-ABE. Lastly, the results indicate that when we use CP-ABE scheme the possibility of attack may be decreased.
When the CB-ABE scheme, combine with OTP and Digital Signature technology. That achieves more strength and establishes secure communication among fog and cloud. Use of combination of these technologies ensures the confidentiality more than other methods. It verifies double times and provides efficient and effective communication.

V.CONCLUSION

Fog computing is one of the promising solutions for handling the big data that is being produced by the IoT, which is often security-critical and time-sensitive. This review discusses about fog computing, several security, security algorithms. Finally, we provided challenges and future directions for research in fog computing. We truly believe that this survey would be a source of inspiration towards research direction to solve different challenges in privacy and security in the fog.

REFERENCES

[1] Mohammad Irshad.," A Systematic Review of Information Security Frameworks in the Internet of Things "in Proc. IEEE 18th Int. Conf. on High Performance Computing and Communications, 14th Int. Conf. on Smart City; 2nd Int. Conf. on Data Science and Systems,2016.

[2] Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. "Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing-MCC '12", *Helsinki, Finland, 17 August 2012; pp. 13–15.*

[3] Yi,S.;Hao,Z.;Qin,Z.;Li,Q ."Fog computing: Platform and applications." *In Proceedings of the3rdWorkshop on Hot Topics in Web Systems and Technologies, HotWeb 2015, Washington, DC, USA, 24–25 October 2016; pp. 73–78.*

[4] Definition of Fog Computing. Available online: *https: // www. Open fog consortium. org/ # defnition- of-fogcomputing* (accessed on 24 March 2018).

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

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 9, September 2018

[6] Ranesh Kumar Naha1 , Saurabh Garg1 (Member, IEEE), Dimitrios Georgekopolous (Member, IEEE), Prem Prakash Jayaraman (Member, Ieee),Longxiang Gao (Senior Member, IEEE), Yong Xiang3 (Senior Member, Ieee), And Rajiv Ranjan(Senior Member, IEEE),” Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions” Available: https://arxiv.org/abs/1807.00976

[7] Takabi, H., Joshi, J.B., Ahn, G.J.”Security and privacy challenges in cloud computing environments” IEEE Security and Privacy 8 (2010)

[8] A. Sahai and B. Waters, “Fuzzy identity based encryption,” in Proc. Acvances in Cryptology—Eurocrypt, 2005, vol. 3494, LNCS, pp. 457–473.

[9] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji. (2016, Nov.). CCAsecure ABE with outsourced decryption for fog computing. Future Generation Computer Systems. [Online]. Available: https://doi.org/10.1016/j.future.2016.10.028

[10] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ‘‘Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

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

[12] J. Hur, ‘‘Improving security and efficiency in attribute-based data sharing,’’ IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Oct. 2013.