INTERNATIONAL JOURNAL OF SCIENTIFIC PROGRESS AND RESEARCH (IJSPR) ISSN: 2349-4689

FOG COMPUTING
Securing the Cloud and its Applications in IOT

[1]Kavana S P, [2]Swathi V S, [3]Ujwal S, & [4]Shivaraja H M
Dept. of CSE & ISE
BGS Institute of Technology

Abstract— Cloud computing will significantly change the way we use our computer & store our personal and public information because of its flexibility and scalability cloud competing is considered as one of the most exciting technology. The threat in cloud is data security. The fog computing is introduced in order to overcome the limitations in cloud computing. The fog computing is associated with the Advanced Encryption Standard (AES) Algorithm. Which is considered to be the most advanced and secured standard for encryption of electronic data. Fog computing is not the replacement of cloud computing, it is defined as cloud computing paradigm. The term "fog computing" or "fogging" describes a decentralized computing infrastructure, where computing resources and application services are brought to the edge of the network introducing a intermediate processing layer between IOT devices and cloud hence fog is a cloud close to the ground. Using fogging entire data over data sets is being accurately encrypted and decrypted vice versa. Fogging has distinctive characteristics in location sensitivity, wireless connectivity and graphical accessibility to create new security and forensics issues and challenges which have not been in cloud security & cloud forensics. The internet of things(IOT) is one of the hottest mega trends in technology, deals with all the components of what we consider web 3.0 including big data analytics cloud computing, fog computing and mobile computing.

Keywords—Cloud Computin, Fog Computing; AES Algorithm; Internet of things(IOT); Encyption and decryption

I. INTRODUCTION

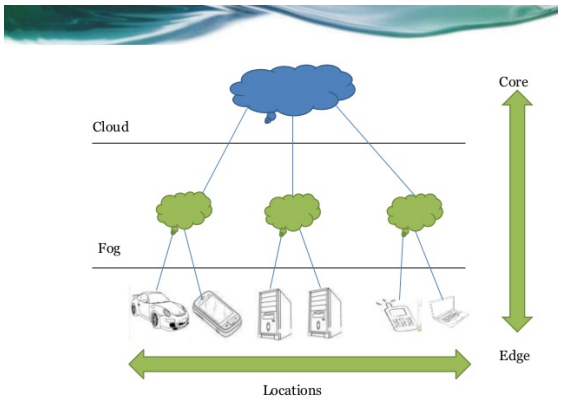

Fig. 1. Basic Diagram

Fogging allows computing, decision making and action taking to happen via IOT devices and only pushes the relevant data to the cloud. CISCO gave brilliant definition for fog computing: "The fog extends the cloud to be closer to the things that procedure and act on the IOT data". The goal of fogging is to improve efficiency and reduce the amount of data transported to the cloud for processing, analysis and storage. This is often done to improve efficiently, though it may also be used for security and compliance reasons. Popular fog computing applications include smart grid, smart city, smart buildings, vehicle network and software-defined network [1]. Now a day every organization from large-scale to small-scale industry depends on the cloud computing technology [2] to store their data and to retrieve the data. As per the survey in the year 2010. The number of devices connected to the internet has exceeded the world's population and it is believed that in the next five years from now it would be above 50 billion of devices connected to the internet increases there will be problem in the storage as well as information retrieval process. The solution for the above problem is fog networking. Fog networking consists of a control plane & a data plane. For example, on the data plane, fog computing enables computing services to reside at the edge of the network as opposed to servers in a data-center. Compared to cloud computing, for computing emphasizes proximity to end users and client objectives, dense geographical distribution and local resource pooling, latency reduction and backbone bandwidth savings to achieve better quality of services(QOS) and edge analytics/stream mining, resulting in superior user-experience and redundancy in case of failure. [2]Fog networking supports the Internet of things(IOT) concept, in which most of the devices used by humans on a daily basis will be connected to each other, examples include phones, wearable health monitoring devices, connected vehicles and augmented reality using devices such as the Google glass [2]. The security will track the user and will map all the data concerned with the user when unauthorized user tries to access the data in the cloud [3]. The characteristics of the fog such as low latency location awareness, white spread, geographical distribution mobility, very large number of nodes and real time application, heterogeneity. These characteristics make the fog the appropriate platform for a number of critical IOT services & applications [4].

II. SURVEY ON FOG COMPUTING

In March 2016, Aatish B Shah, ET. Al [5] published paper with a topic "Fog Computing: securing the c are loud and preventing insider attacks in the cloud". They explained about ultra-cloud, wargaming.net, user behavior profiling, decays and modules. In modules they are discussed about user authentication, admin module, file access module, data access module and decay module. Then in March 2010, Muhammad Kazim University of Derby, United Kingdom Shao ying university of Derby, United kingdom, Published a paper on the topic "cloud security Alliance", "Top threat to cloud computing VI.0". According to this paper, cloud computing offers many advantages such as increased utilization of hardware resources, scalability,

reduced costs and easy deployment. As a result, all the major companies including Microsoft, Google and amazon are using cloud computing. Moreover, the number of customers moving their data to cloud services such as indeed, Google Drive, Drop box, Facebook & LinkedIn is increasing every day. In October 2016, Vinod pande, Chethan Mahlecha, and Sangram Singh Kayte published a paper on topic "Fog computing and its role in the internet of things". Where they discussed about the applications like smart grid, wireless sensors and actuators networks and open challenges and future directions.

III. WHAT HAPPENS IN FOG AND THE CLOUD

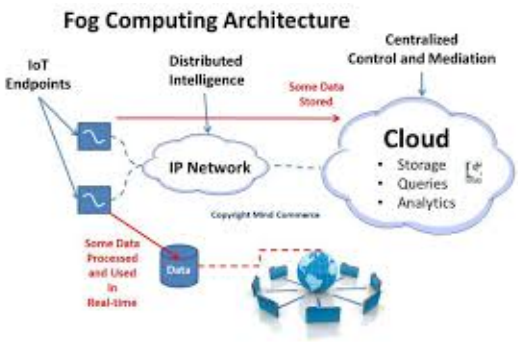

Fig 2. Fog Computing Architecture

There are many security issues in cloud computing as of man in the middle attack and even the encryption of data is not safe method for cloud. It doesn't recognize the difference between user and attacker and it is less concentrated on the security of data. One of the examples for data theft in the cloud is twitter. For storing and accessing of the data cloud gives various services in which the main theft is that failure to provide security for the data against attackers. Here comes the existence of the fog computing which is concerned to be the most secured forms of data storage. Fogging uses decoy system as security system for authorization of data. This decoy system method has been incorporated with user behavior profiling, when any unauthorized access will be notified to the system. In decoy system firstly user has to sign up and then the login details and once he had logged in, he needs to answer the security questing which was given while creating an account. But in this method while answering there is risk that the attacker might guess the security questions. To avoid this introduced a solution by Advanced Encryption Standard (AES) algorithm where data will be encrypted so that even if the attackers want to access the data from present decoy system this makes him difficult to access the data. Whatever the data given by the user is directly stored in the cloud. So, this may lead unsecure of data, but in fog computing the data will be encrypted by any codes and it is stored in the cloud and it will decrypted in retrieval process. By this our data will be secured and confidential.

FOG NODES:

- Using any protocols receive feeds from IOT devices, in real time.
- With mille second response time seen IOT enabled application for real time control and analytics.
- Provide transient storage, after 1-2 hours.
- Periodic data summaries send to the cloud.

THE CLOUD PLATFORM

- [6]The data summaries are received and aggregated from many fog nodes.
- Analysis is performed on IOT data and data from other sources to gain business insight.
- Based in these insights can send new applications servers to the fog nodes [6].

□V.□□ W DOES THE FOG WORKS?

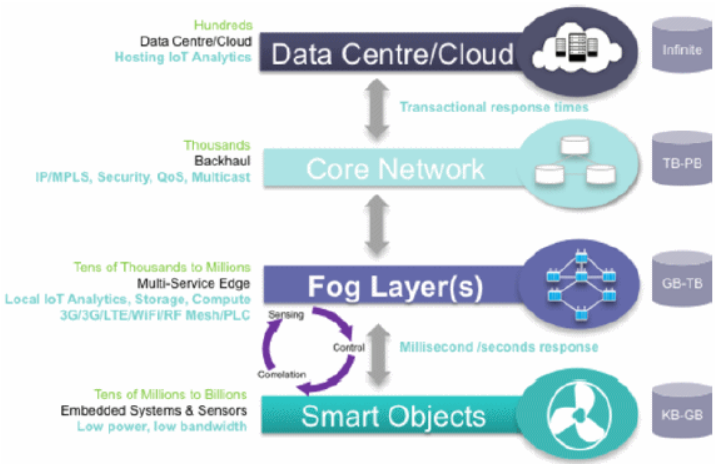

Fig 3.Three layer architecture of fog computing.

The basic fundamental components of this architecture are called fog nodes. They are an array of modular hardware and software elements that can be configured to execute specific functions. Fog computing performs following actions to make edge of the network:-

1) Adding process and memory resources to edge devices.

2) Pre processing collected data at the edge.

3) Sending aggregated results to the cloud.

It is essentially, a middle layer between the cloud and the hardware to enable more efficient data processing, analysis and storage, which is achieved by reducing the amount of data which needs to be transported to the cloud. Device

communicates peer to peer within a fog domain and through cloud across fog domains.

Table 1. Relation between Fog nodes and Cloud

	Fog nodes closest	Cloud	Fog nodes
Application examples	Smart grid, open fog consortium	□g data analytics	Visualization
Response time	Mille sec to sub sec	Days-Weeks	Sec-Minutes
How long IOT data is stored	Short duration	Hours, days or weeks	Months or years
Geographical coverage	One city	Global	Wider

- [6]In fog computing the most time sensitive data is analyzed on the fog nodes. For example in CISCO smart grid distribution network, the most time sensitive requirement is to verify that protection and control loops whether operating properly [6].
- The less time sensitive data is sent to cloud for historical analysis. For example each of thousands of fog nodes sends periodic summaries of grid data to the cloud for storage and analysis.

V. HOW CAN WE SECURE DATA IN CLOUD BY FOG?

The main problem that we face in cloud computing is security, it can be overcome by fog computing as it is incorporated with advanced encryption standard algorithm.

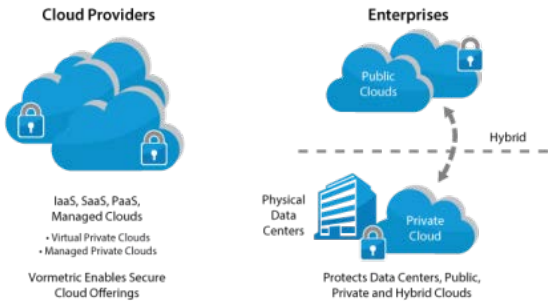

Fig 4. Securing cloud

Table 2. Specification of AES

	General
Designers	Vincent Rijmen, Joan Daeman
First Published	1998
Derived from	square
Successors	Anubis, Grand cru
certification	AES winner, CRYPTREC, NESSIE, NSA, Cipher details
Key sizes	128,192 or 256 bits
Block sizes	128 bits
structure	Substitution-permutation network
rounds	10,12 or 14 (Depending on key size)

AES is based on design principle known as substitution permutation network combination of both substitution and permutation, and it is fast in both software and hardware. It operates on a 4x4 column major order matrix of bytes termed the state. Most AES calculations are done in a particular finite field.

For example, if there are 16 bytes, {\display style b_{0},b_{1}…b_{15}}, these bytes are represented as this matrix:

{\display style

{\begin{bmatrix}b_{0}&b_{4}&b_{8}&b_{12}\\b_{1}&b_{5}&b_{9}&b_{13}\\b_{2}&b_{6}&b_{10}&b_{14}\\b_{3}&b_{7}&b_{11}&b_{15}\end{bmatrix}}}

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the cipher text. The number of cycles of repetitions is as follows:

- 10 cycles of repetition for 128 bit keys.
- 12 cycles of repetition for 192 bit keys.
- 14 cycles of repetition for 256 bit keys.

[7]Each round consists of several processing steps, each containing four similar but different stages, including one

that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key [7].

Privacy: Privacy plays major role in fog computing, because fog nodes are in vicinity of endorsers and collect more sensitive information than the remote cloud lying in the core network. Some of the privacy preserving techniques are: data privacy, usage privacy, location privacy etc.

VI. WHY THE IOT NEEDS FOG COMPUTING?

1) *Function allocation*

Same like cloud fog is also an architecture. Not only for one application domain it has function allocation for many applications. As opposed to resources fog efficiently distributes the allocation of functions in IOT networks. This helps to simplify and standardize fundamental global IOT network operations such as configurations and management.

2) *Distributed architecture*

The distributed architecture provides value throughout the networks, not just at the edge. Fog distributes communication, storage and control flexibly.

3) *Immersive distribution*

The immersive distribution offers centralization, it means fog resources are available throughout the network. It enables the flexibility.

4) *Scale*

For security, cognition, agility, latency and efficiency scale is the open fog acronym.

5) *Latency*

Fog services have small and deterministic latency that enables real time systems such as virtual reality, artificial intelligence, real time control loops and more.

VII. FOG COMPUTING APPLICATIONS IN IOT

"For computing works well in cloud-based control plane to provide control and broader insight across a large numbers of nodes". These include transportation, agriculture, wind energy, surveillance smart cities and buildings.

I. Smart cities and fog computing

[8]Larger cities face challenges from traffic congestion, public softly, high energy use, sanitation and in providing municipal services. These challenges can be addressed within a single IOT network by installing a network of fog nodes [8]. Fog Computing architecture allows for fog nodes to provide local processing and storage. This optimizes network usage along with this smart cities also struggle with safety and security, where for computing address security, data encryption and distributed analytics requirements.

II. Smart buildings and fog computing

A commercial building may contain thousands of sensors to measure various building operating parameters: temperature, key card headers and par node king space occupancy. Data from these sensors is analyzed, such as triggering a fire alarm if smoke is sensed, fog networking allows for local operations for optimized control function.

Each wing or even individual room could contain its own fog node that is responsible for performing emergency monitoring and response functions, controlling climate and lighting, and providing a building resident compute and storage infrastructure to supplement the limited capabilities of local smartphones, tablets and computers.

III. Open fog Consortium

Table 3: Open fog consortium

Type	Consortium
Industry	telecommunication
Founded	19 November 2015
Founders	Cisco Systems Intel Microsoft Princeton University Dell ARM Holdings
Headquarters	Fremont, California
Key people	Chairman of the board Helder antunes President Jeff Fodders
Website	Openfogconsortium.org

[7]The open fog consortium is a consortium of high tech industry companies and academic institutions across the world aimed at the standardization and promotion of fog computing in various capacities and fields [7].

[9]The open fog consortium is a global non preformed in order to solve the bandwidth, latency, communications and security challenges associated with IOT, and artificial intelligence. [9]

VIII. ADVANTAGES/BENEFITS OF FOG COMPUTING

- [10]Fog computing enables a single, powered processing device to process data received from multiple end points and send information exactly where it is needed [10].

- It offers lower latency than a cloud.
- Fogging is more scalable as it was multiple data points feeding it information.
- Cost: Fog computing requires significantly less movement of data which frees up the network for other use.
- Latency: Fog based IOT applications such as vehicle to vehicle communication receives the least amount of latency as possible.
- [11]Encapsulation: Data, application, services, storage, computing power analytics, networking and other are encapsulated in fog computing paradigm [11].
- Expense: Fogging process the data locally instead of sending it to cloud so, conserve network bandwidth.
- Privacy control: Analyze the data locally instead of sending it to cloud.
- Security: secure the data, as it is using AES Algorithm.

IX. CONCLUSION

We can see fog computing as a new paradigm or as made up of marketing hype, we will probably encounter the term over the next few years as the IOT gains attraction. Fog computing takes some of the heavy lifting of regular cloud services by utilizing local resources for quicker and smoother processes. Whatever the devices connected to your organizations network, it helps you to provide the management and service support required to keep your entire IT infrastructure running smoothly. The fog is just another word for cloud plus IOT. This would allow, say smart devices to send software updates to each other rather than sending them through the cloud first.

X. ACKNOWLEDGEMENT

This research was supported/partially supported by Divya Mam, Assistant prof Dept. of CSE and ISE, BGS Institute of Technology & Nithin Sir, Assistant prof Dept. of CSE and ISE, BGS Institute of Technology. We thank our Staff from BGS Institute of Technology, BG Nagar who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.
We would also like to show our gratitude to the B K Narendra Sir, The Principle, BGS Institute of Technology & Shashikala Mam, Head of Department, Dept. of CSE & ISE, BGS Institute of Technology for providing us opportunity to participate in National Conference

REFERENCES

[1]https://internetofthingsagenda.techtarget.com/definition/fog-computing-
Fogging

[2] https://en.wikipedia.org/wiki/Fog_computing

[3] Ryoichi Sasaki and Tefsubaro Uehara, Fog computing: Issues and
Challenges in security and forensics Cambridge University press,
Cambridge 1982.0730-3157/15 2015 IEEE.

[4] www.techrepublic.com/whitepapers

[5] Aatish B shah, Jai Kannan, Deep Utkal shah, Prof S B ware, Prof R S Badodekar, Department of Information Technology. Singad Institute of Technology Lonavala. "Fog computing: securing the cloud and preventing insider attack in the cloud"

[6] CISCO system. In charge, San Jose, CA, "Fog computing and internet of things: extend the cloud to where the things are".

[7] https://em.m.wikipedia.org/wiki/advanced-encyption-standard

[8] https://www.networkworld.com/article/317085/internet-of-things/which- iot-applications-works-best-with-fog-computing.html

[9] info@openfogconsortion.org

[10] readwrite.com/2016/08/05/fog-computing-different-edge-computing-p11/

[11] www.dataversity.net/the-future-of-cloud-computing-and-the-internet-of-things/