A COMPARATIVE STUDY OF CLOUD AND FOG COMPUTING

[1] Rosy Bhumrah,[2] Ankit Bansal,[3] Diksha Rani , [4] Harsimranpreet Kaur
[1]Assistant Professor, [2] Associate Professor, [3] Assistant Professor, [4] Assistant Professor
[1]Department of Computer Science & Engineering
[1] Gulzar Group of Institutes, Ludhiana, India

ABSTRACT - In this contemporary era, although with the increasing usage of cloud computing, there are still some challenges which are unresolved such as real time latency, lack of mobility support, low capacity, network failure etc. Fog computing can deal with these problems by providing expandable resources and services to the end users, at the edge of network, while cloud computing are more about providing resources distributed in the core network. Generally, Fog computing resides closer to the devices that extend the Cloud-based computing, storage and networking facilities. These devices, called fog nodes, can be deployed anywhere with a network connection: on a factory floor, on top of a power pole, alongside a road or train track, in any automobile vehicle. Any device with computing, storage, and network connectivity can be a fog node. In this comparative study, we elaborate the comparison among cloud and fog on the basis of some parameters like security and privacy issues, data processing, architecture etc. and Finally, this paper also enlighten how fog computing have cutting edge over cloud computing.

Index Terms: Cloud Computing, Fog Computing, Fog Nodes, Real-time latency, Mobility support.

I. INTRODUCTION

Now a day, as most of the information about emails, bank account details, personal information stored on different social media sites are accessible through different gadgets and mobile devices in a single click. All this could happen due to cloud. Cloud computing refers to the ability to store and retrieve data from off-side locations. However, slow bandwidth is secretly contributing to the increase in restrictions of a wireless network. 3G and 4G cellular networks are not proficient enough to transmit data from devices to the Cloud at the same speed that the data is generated. Thus, CISCO recently delivered the vision of fog computing to enable applications on billions of connected devices to run directly at the network edge and hence, fog computing is also known as *Fogging or Edge Computing*.

Since Cloud data centers are geographically centralized, they often fail to deal with storage and processing demands of billions of geo-distributed devices. Fog computing facilitate location information, mobility support and real-time interactions. Fog and cloud computing are interconnected. In nature, fog is closer to the earth than clouds; in the technological world, it is just the same, fog is closer to end-users, bringing cloud capabilities down to the ground. The main task of fog is to deliver data and place it closer to the user who is positioned at a location which at the edge of the network. Fog can also include *cloudlets* — small-scale and rather powerful data centers located at the edge of the network. Their purpose is to support resource-intensive apps that require low latency. The main difference between fog computing and cloud computing is that cloud is a centralized system, while fog is a distributed decentralized infrastructure.

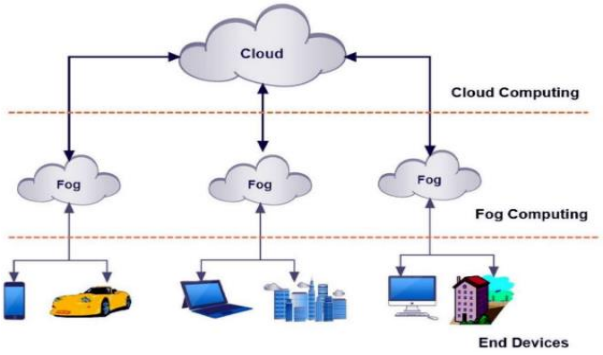

Fig.1: Fog between Cloud and End Devices

As shown in fig.1, Fog computing is a mediator between hardware (End Users) and remote servers. It regulates which information should be sent to the server and which can be processed locally. In this way, fog is an intelligent gateway that offloads clouds enabling more efficient data storage, processing and analysis. One should note that fog networking is not a separate architecture and it doesn't replace cloud computing but rather complements it, getting as close to the source of information as possible. The new technology is likely to have the greatest impact on the development of IoT, embedded AI and 5G solutions, as they, like never before, demand agility and seamless connections.

II. PROS AND CONS OF BOTH TECHNOLOGIES

Pros of Cloud Computing

Since connected devices have limited storage capacity and processing power, the integration with cloud computing comes to support:

- **Improved performance** (the communication between IoT (Internet of Things) sensors and data processing systems is faster)
- **Storage capacities** (highly scalable and unlimited storage space are able to integrate, aggregate and share the enormous amount of data)
- **Processing capabilities** (remote data centers provide unlimited virtual processing capabilities on-demand)
- **Reduced costs** (license fees are lower than the cost of the on-premise equipment and its continuous maintenance)

Pros of Fog Computing

However, fogging approach has many benefits for the Internet of Things, Big Data and real-time analytics. Some of the main advantages of fog computing over cloud computing are as given below:

- **Low latency** (fog is geographically closer to users and is able to provide instant responses)
- **No problems with bandwidth** (pieces of information are aggregated at different points instead of sending them together to one center via one channel)
- **Loss of connection is impossible** (due to multiple interconnected channels)
- **High security** (because data is processed by a huge number of nodes in a complex distributed system)
- **Improved user experience** (instant responses and no downtimes satisfy users)
- **Power-efficiency** (edge nodes run power-efficient protocols such as Bluetooth, Zigbee or Z-Wave)

Cons of Cloud Computing

Unfortunately, there is nothing immaculate, and cloud technology has some downsides, especially for the Internet of Things services.

- **High latency** (more and more IoT apps require very low latency, but cloud can't guarantee it because of the distance between client devices and data processing centers)
- **Downtime** (technical issues and interruptions in networks may occur for any reason in any Internet-based system and make customers suffer from an outage; many companies use multiple connection channels with automated failover to avoid problems)
- **Security and privacy** (your private data is transferred through globally connected channels alongside thousands of gigabytes of other users' information; no surprise that the system is vulnerable to cyber attacks or data loss; the problem can be partially solved with the help of hybrid or private clouds)

Cons of Fog Computing

On the other hand, In case of Fog, the technology doesn't have any apparent disadvantages, but some shortcomings can be given as below:

- **A more complicated system** (fog is an additional layer in the data processing and storage system)
- **Additional expenses** (companies should buy edge devices: routers, hubs, gateways)
- **Limited scalability** (fog is not as scalable as cloud)

III. SECURITY AND PRIVACY ISSUE IN CLOUD AND FOG COMPUTING

Various methods are implied for securing data on cloud server by using different type of techniques. Sometimes this technique fails or is unsuccessful in securing user cloud data from insider attacks and sometimes other reason also come into picture such as, misconfiguration of services etc.

1. ***User Behavior Profiling****:* User profiling is a well-known technique that can be applied here to how, when and how much a user accesses their information from cloud database. The system continuously monitors user behavior to check whether the pattern is normal or else abnormal access or unauthorized access to user information might be in action. Each user has a distinct profile consisting of number of times the user has accessed his files from cloud server. If there is any divergence in user behavior against the profile which is already stored in database, then it can be identified as an invalid user and attack is detected.

2. ***Decoys:*** Decoy information are the fake documents, trap-files, honey-files and other fake information that are uploaded by cloud system administrator on system. Fake information contains all false data which create confusion to attacker. This technique is incorporated along with user behavior profiling. When unauthorized access is identified then disinformation attack is launched and decoy data base starts providing fake data to particular user in such a way which is completely legitimate or legal or normal. Only true owner user of data can identify when fake data is provided by cloud data base then real user can ask one-time password for verification. This secures users actual data on cloud and protects it from misuse of real data by unauthorized user. Fig. 2 depicts the concept of decoy in cloud computing.

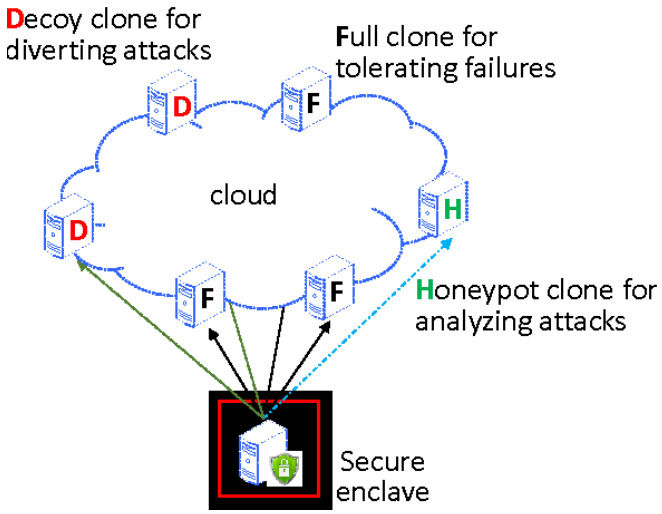

Fig. 2: Decoy implementing in cloud computing

However, the main security issue in fog is *authentication* since services are provided to the end users by front fog nodes. Many authentication techniques applied for fog computing to provide an efficient authentication but some of them not efficient and have poor scalability such as Traditional PKI-based. Also biometric authentication techniques applied to provide an efficient authentication such as face authentication, fingerprint authentication, touch-based authentication or keystroke-based authentication.

One of the typical attack in fog computing is ***Man-in-the Middle attack***. The idea of Man-in-the-Middle attack is replacing the gateways that serving the fog device by fake one which is connecting to malicious access points. In this case, any private communication of victims will be hacked and thus the gateways will be controlled by the attackers. The attacker will be able to monitor and modify the data between end user and gateway. Figure 3 show an example of man-in-the-middle attack which shows the ability of the attacker to monitor and modify the data that is sending from user with a 3G connection to another user with WLAN connection in the middle of the communication. Traditional method faces difficulties to detect man-in-the-middle attack without noticeable features of this attack collected from the fog because this attack consumes a small amount of fog devices, such as memory and CPU consumption.

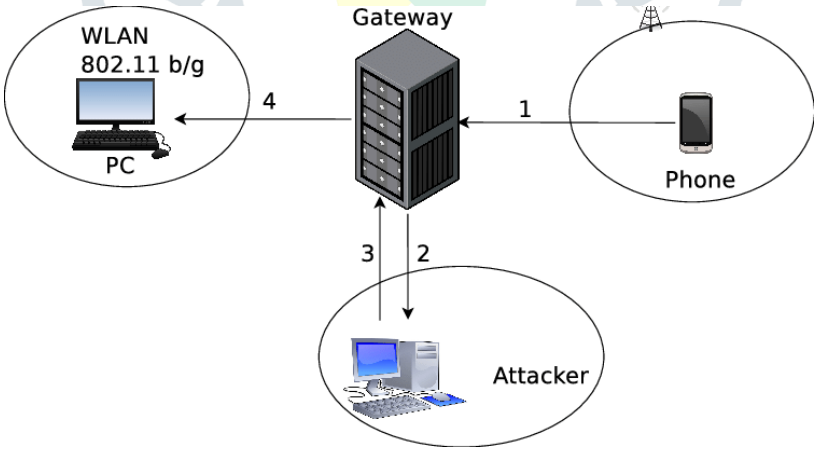

Fig.3: Man-in-the-Middle attack in Fog Computing

IV. COMPARISON CHART OF CLOUD VS FOG COMPUTING

Fog is a form of cloud that lies low on or near ground level. Table 1 shows the differences between cloud computing and fog computing on the basis of different parameters and requirements:

Table 1: Differences between cloud computing and fog computing

Requirement	Cloud Computing	Fog Computing
Server nodes location	Within the Internet	At the edge of the local network
Client and server distance	Multiple hops	Single hop
Latency	High	Low
Delay Jitter	High	Very low
Security	Less secure, Undefined	More secure, Can be defined
Awareness about location	No	Yes
vulnerability	High probability	Very low probability
Geographical distribution	Centralized	Dense and Distributed
Number of server nodes	Few	Very Large
Real time interactions	Supported	Supported
kind of last mile connectivity	Leased line	Wireless
Latency	It has low latency	It has low latency in terms of network
Capacity	It does not provide any reduction in data while sending or transforming data	It reduces the amount of data sent to cloud computing.
Bandwidth	It conserves less compared with Fog Computing	It conserves the amount of bandwidth.
Responsiveness	Response time of the system is low.	Response time of the system is high.
Security	High but less compared to Fog Computing	High Security.
Speed	Access speed is high depending on the VM connectivity	High even more compared to Cloud Computing
Data Integration	Multiple data sources can be integrated.	Multiple Data Source and devices can be integrated.

V. CONCLUSION AND FUTURE SCOPE

Fog computing is an extended cloud for smart devices working at edge of the network which aims to process and analysis data before sending to the cloud. Fog stays in the middle between devices and cloud in which it can provide more secure and private communication with other additional features that are not included in the cloud. During our comparative study we observe that Fog computing has low latency and provides high response rate and has become most recommended compared to cloud computing. It supports the Internet of Things as well as compared to Cloud Computing. In terms of large users and widely distributed networks, Fog computing is preferred and recommended to get more efficiency and high productivity.

Further, in terms of security attack, fog prevents the unauthorized access problem of data and information. In our comparative study we observed the main issue faced in the fog which is man-in-the-middle attack. This attack enables the attacker to replace the service that serve specific device with fake one. With fog computing, we not only prevent the attack but also if the end user faced a fake page, he will not be affected because the password will be generated with every login and deleted with every logout. The attacker will not get any benefit from his fake page because the fake page will not be connected to the cloud and password will generated in the cloud and sent to the user through SMS service by service provider. This solution can be improved in the future with other features.

REFERENCES

[1] Parashar Sangle, Romit Deshmukh, Rohit Ghodake, Akash Yadav, Prof. Jitendra Musale, 2017, "***Data Security System in Cloud by Using Fog Computing and Data Mining***", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 7, Issue 3, March 2017.

[2] Er. Pummy Dhiman, 2017, "***FOG COMPUTING-Shifting from Cloud to Fog***", International Journal of Engineering Science and Computing, March 2017, Volume 7 Issue No.3.

[3] Ivan Stojmenovic, Sheng Wen , 2014,"***The Fog Computing Paradigm: Scenarios and Security Issues***", Proceedings of the 2014 Federated Conference on Computer Science and Information Systems pp. 1–8, ACSIS, Vol. 2.

[4] 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, ser. MCC'12. ACM, 2012, pp. 13–16.

[5] Cisco, "***Cisco delivers vision of fog computing to accelerate value from billions of connected devices***," Cisco, Tech. Rep., Jan. 2014.

[6] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the internet of things," in *Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing*, ser. MCC'13. ACM, 2013, pp. 15–20.

[7] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[8] L. Zhang, W. Jia, S. Wen, and D. Yao, "***A man-in-the-middle attack on 3g-wlan interworking***," in Communications and Mobile Computing (CMC), International Conference on, vol. 1, April 2010, pp. 121–125.

[9] Bansal A, et al; "A Comparative Analysis of Cloud Computing with Grid Computing", International Journal of Advance Research and Innovation (ISSN 2347 – 3258)(2017)

[10] S. Sarkar, S. Chatterjee, S. Misra,"***Assessment of the suitability of fog computing in the context of internet of things***", IEEE Transactions on Cloud Computing", 2015

[11] M.Redowan and B. Rajkumar," ***Fog Computing: A Taxonomy, Survey and Future Directions***",Nov. 2016

[12] Sandeep Kaur, Er. C.K.Raina, 2017**, "Survey Paper on Fog Computing",** International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2 | Issue 3

[13] Ben-Salem M., and Stolfo Angelos D. Keromytis, "***Fog computing: Mitigating Insider Data Theft Attacks in the Cloud***," IEEE symposium on security and privacy workshop (SPW) 2012.

[14] 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, ser. MCC'12. ACM, 2012, pp. 13-16.

[15] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "***A view of cloud computing,***" Commun. ACM, vol. 53, no. 4, pp. 50-58, Apr 2010.