

Fogging: An Advanced Version of Cloud Storage

Md. Tareq Hasan

Senior Lecturer

Department of Computer Science
& Engineering,
University of Development
Alternative, Dhaka, Bangladesh

Md. Mustafijur Rahman

Teaching Assistant

Department of Electrical &
Electronic Engineering,
Manarat International University,
Dhaka, Bangladesh

Rajib Chakrabarty

IT Officer

Shimizu Corporation
Bangladesh Office
Dhaka, Bangladesh

ABSTRACT

In the new era of digital world, cloud computing has become the traditional way of data storage. In this paper, we are going to introduce a new technology which is known as fog computing. Fog is used for high security and protection of big data. The main concentration is for processing here.

Keywords

IoT, Cloud computing, Fog computing.

1. INTRODUCTION

Now a day the use of cloud computing to store big amount of data for different purposes are increasing. Day by day cloud computing is growing up rapidly with its higher popularity. Huge number of services is provided to the users by cloud computing. It is convenient and on demand network access to a pool which is shared of configurable computing resources [1].

Because of all this reasons, software companies are drifting to this technology. Since a lot of users are now in this arena, data integrity, security and confidentiality is getting risky. Cloud computing is not just a used model earlier, it is a combination of many computing strategies, number of methodologies, concepts like software related architecture, virtualization to form a virtual pattern, togetherness of fog and cloud, using virtual resources. In this cloud, we have authentication, security mechanisms like identity, authorization, password policies, server roles, but all these are not enough for our security terms. Our data security is consisted with high decryption technologies or the issues of hacking. This is how the concept of Fog computing came into Limelight. The term Fog computing is known as fogging and Edge computing, is a model where data and all applications are mostly concentrated in end users or devices i.e. at the network edge rather than focusing on cloud. Cloud computing can be a proficient contrasting option to owning and keeping up PC assets and applications for some associations, especially little and medium measured associations, because of the compensation as-you-go show and different attributes (e.g., on-request, self-benefit, asset pooling and fast flexibility). In fog configuration, the versatile assets of cloud are stretched out to the edge of the whole system, for example, compact gadgets, wireless sensors and all IoT gadgets to become less inertness and system clogs. IoT gadgets are utilizing interconnected advances like Radio Frequency Identify (RFID), Wireless Sensors and Actor

Networks (WSAN) trading data through the Internet and are more coordinated in our day to day life [1]. Smart cities and farming, Smart grid, keen city, jet engines, brilliant matrix, flying drones, illegal fishing, power grid etc. As Internet of Thing is the smart and innovative technology used these days

for modern home appliances, embedded software systems, needed sensors and many network based applications to communicate with data, using Fog computing would be an extra advantage.

These IoT products made our lives convenient by constrained capacity, higher productive capability, security issues and unwavering quality. Hence, its applications are requiring geo-dispersion, portability bolster, mindfulness of location and lesser inactivity to effectively gather and process information from Internet of Thing gadgets which are providing the characteristics of Fog computing which is like Streamlining, geo-identification, mindfulness of location, arrangement of edge etc. with versatility. Although Cloud and Fog computing almost share common highlights but Fog remained like dominant thereby extending the features and mechanism of Cloud computing.

2. LITERATURE REVIEW

As the majority of present systems are most likely cloud centric, the basic characteristics used with these system is “Device to Cloud” communication and Analysis is completely with the cloud computing or Fog computing or Fogging or Fog Networking is the word which is coined by the CISCO in the month of January, 2014, which refers to extend the Cloud Computing to the edge of the network of the company. It is an architecture which uses one or more end-user clients or edge devices collaboration to function considerable storage amount. Fog figuring is the arena which renders like services to the network system edge. It uses the cloud along with the fog assets for its own foundation, as shown in Figure 1. Devices at the end users use the data, process the data and hence gets retrieved it back at the edge of the network. To have a good and clear idea about the edge devices of cloud network figure1 can be referred. Therefore, instead of fetching the data from very far above from the cloud, the data is directly brought back to the clients using from the nearby devices on the ground (i.e. here fog devices are meant)

Whatever the IoT information be, it is locally managed by gadgets at edge or the close clients to complete a significant measurement of the capacity, correspondence and services. It also observes client portability, needed asset and interface heterogeneity. Fog processing is suitable for the land transportation of assets as to oppose to have an incorporated one, that depicts that “Fog registering is the enhancement of Cloud figuring”. The difference between these two is that Fog gives closeness to its End clients by providing thick land appropriation and by underpinning versatility. The end gadgets used are the Access focuses or set- up boxes to enjoy the services of Fog computing. To know the hierarchy of this three tier system and representation, figure 2 can be referred.

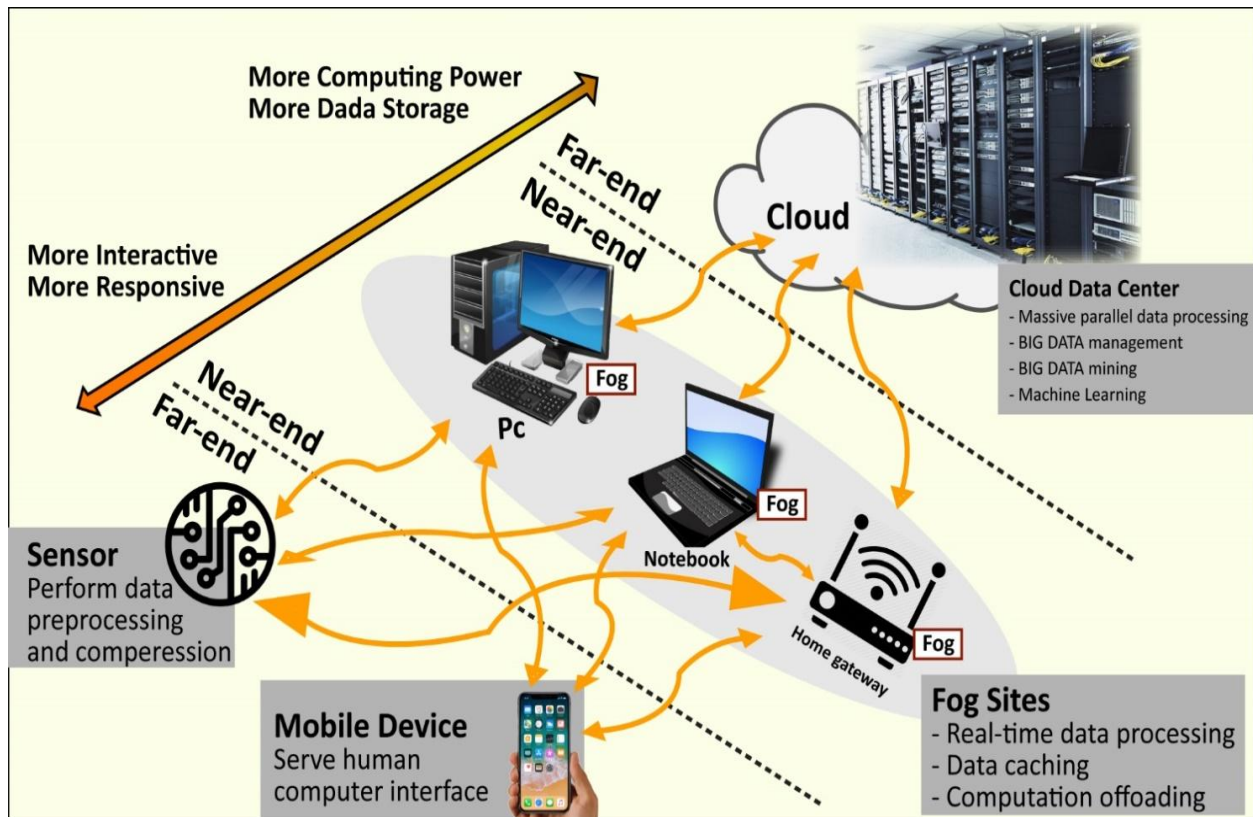


Figure 1: Fog Computing Architecture

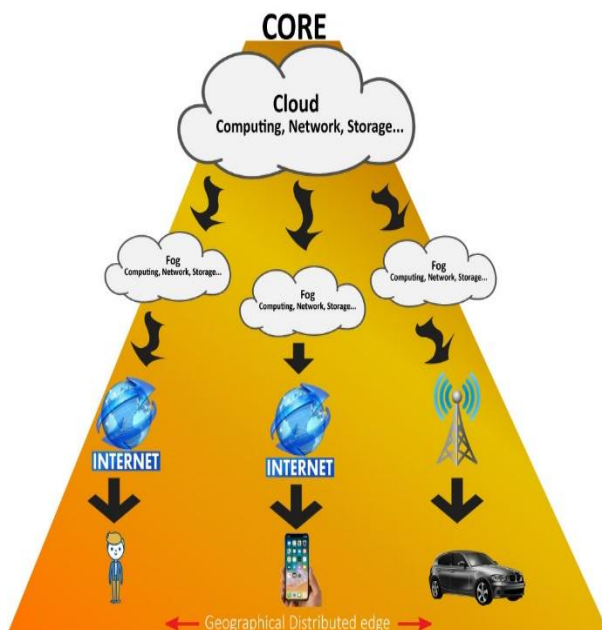


Figure 2: Hierarchy of networks

3. EXISTING SYSTEM

THREATS IN CLOUD: DATA BREAKS- security of the data is leading to risk when any theft occurs during processing.

ACCOUNT OR SERVICE TRAFFIC HIJACKING- for instance, if the login is lost then the account is at risk.

DATA LOSS- the data can be lost, if it is found by the intruder.

ACCOUNT OR SERVICE TRAFFIC HIJACKING- for instance, if the login is lost then the account is at risk.

DENIAL OF SERVICE- sometimes the server is very much overloaded then many millions of people try to access the same service and it could be caught by the hacker.

INSECURE API's- API, called as Application Programming Interface controls most of the third party applications and verify the user, this can be Hazardous sometimes if the third party is there from unknown source.

MALICIOUS INSIDERS- sometimes we don't have any idea when a second person passively attacks by knowing our confidential information of login.

ABUSE OF CLOUD SERVICES- by trying all the services to unblock an account or database the attacker somehow breaks the encrypted information in very short time.

SHARED TECHNOLOGY- sometimes knowing or unknowingly the firms are getting into Cloud then without their knowledge they would be in partner to some other web site.

CONNECTIVITY- an assumption could be made that a device is always connected to the cloud.

OTHERS- connectivity cost, latency, bandwidth and delay jitter are also some important cloud centric assumptions.

So the cloud computing system is a computing that depends on sharing resources of computing rather than using the local servers or any edge devices to handle applications.

So there is an availability of some other companion to help Cloud to perform better even at the end user and this could be achieved by Fog computing in some ways.

4. PROPOSED SYSTEM

In this paper we are proposing a distinct and robust approach to secure data in Cloud which is done by Fogging. Basic characteristics and key specifications of fog computing:

- Heterogeneity: It says that the Fog nodes can be deployed in a wide variety of environments .e.g. smart cars are connected through IoT.
- Interoperability: Fog components are interoperable in order to provide wide range of services like Streaming.
- Real-time communication: It conveys the speedy service also e.g. constant movement observing frameworks, request continuous handling capacities as opposed to clump preparing.
- Geographical distribution: The services and applications objective of the fog is distributed widely.
- Mobility support: Provides the techniques of mobility like decouple host identity to location identity.
- Prevalence to wireless access: Wireless access focuses and cell versatile door are normal cases for fog organized node.
- Low latency and location awareness: Low delay in accessing data and edge location has less inertness.
- Large-scale sensor networks: This is relevant when checking the nature utilizing some circulated frameworks that require suitable assets.

The clear representation of the requirements for cloud computing versus fog computing is as shown in the table below:

Table 1: FOG Vs CLOUD

Requirements	Cloud Computing	Fog Computing
Latency	High	Low
Delay Jitter	High	Very Low
Location Of Service	Within the Internet	At the edge of the local Network
Distance between client and server	Multiple hops	One hop
Security	Undefined	Can be defined
Arrack on data enroute	High Probability	Very low probability
Location Awareness	No	Yes
Geo-distribution	Centralized	Distributed
No. of server Nodes	Few	Very Large
Support for Mobility	Limited	Supported
Real time Interaction	Supported	Supported
Type of last mile connectivity	Leased line	Wireless

Hence with the seamless integration of both the cloud and the fog services, we are ready to improve the enrolment by disconnecting client information to stay on the edge.

5. APPLICATIONS

1. The most used application is extending cloud computing.
2. In the field of Internet of thing, in various applications like Smart city, Smart grid, digital city, keen city, Smart farming, Robotics with IoT etc.
3. Fog is use reliable and friendly.
4. Enables all real-time analytics.
5. It is so much securable, strongly dependable and adaptable too.
6. Though it enables third party's applications to access user's information, the data is sometimes predictable to outsiders but still this can be solved with the use of dependable protocols.

6. CONCLUSION

In the conclusion an advanced technique to secure data in cloud through fogging is proposed. In this paper author come up with fog computing and it gave advancement to the existing methodologies of securing data in cloud.

7. FUTURE SCOPE

In this paper a new scope of fog computing in future is discussed. We will come up with many more advancement in this technology. No doubt about the fact that there will be a foggy future ahead.

8. REFERENCES

- [1] Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud, USA
- [2] 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.
- [3] Ben-Salem M., and Stolfo, "Decoy Document Deployment for Effective Masquerade Attack Detection," Computer Science Department, Columbia University, New York.
- [4] F. Bonomi, "Connected vehicles, the internet of things, and fog computing," in The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA, 2011.
- [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, ser. MCC'12. ACM, 2012, pp. 13-16.
- [6] 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.
- [7] C. Wei, Z. Fadlullah, N. Kato, and I. Stojmenovic, "On optimally reducing power loss in micro-grids with power storage devices," IEEE Journal of Selected Areas in Communications, 2014 to appear.

- [8] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.
- [9] K. Liu, J. Ng, V. Lee, S. Son, and I. Stojmenovic, "Cooperative data dissemination in hybrid vehicular networks: Vanet as a software defined network," Submitted for publication, 2014.
- [10] K. Kirkpatrick, "Software-defined networking," *Commun. ACM*, vol. 56, no. 9, pp. 16-19, Sep. 2013.
- [11] Cisco, "Cisco delivers vision of fog computing to accelerate value from billions of connected devices," Cisco, Tech. Rep., Jan. 2014.
- [12] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenw_ülder, and B. Koldehofe, "Opportunistic spatio-temporal event processing for mobile situation awareness," in *Proceedings of the 7th ACM International Conference on International Journal of Engineering Science and Computing*, March 2016 2709 <http://ijesc.org/> Distributed Event-based Systems, ser. DEBS'13. ACM, 2013, pp. 195-206.
- [13] H. Madsen, G. Albeanu, B. Burtschy, and F. Popentiu-Vladicescu, "Reliability in the utility computing era: Towards reliable fog computing," in *Systems, Signals and Image Processing (IWSSIP)*, 2013 20th International Conference on, July 2013, pp. 43-46.
- [14] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenw_ülder, 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.