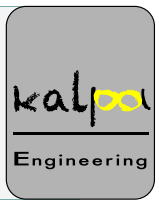
Kalpa Publications in Engineering

Volume 2, 2018, Pages 89–94

Proceedings on International Conference on Emerging Trends in Expert Applications & Security (2018)



Reliability in Fog Computing

Manu Sharma
Gyan Bihar School of Engineering & Technology
Electronics & Communication Department
manu.sharma1988@yahoo.com

Abstract

In the world of Digital Innovation "Cloud Computing" is not just a word or a technology but a paramount to the organizations now days. Because it is not easy to store, compute the data on an internet and central remote server to manage a huge bulk of data and information. It is well known that cloud computing provides data, storage of data, computation of data to the end user also by providing the services to the end users by the different applications. So, now the Fog Computing Is generally a concept to extend the cloud computing technology as it also does the same function which cloud computing functionality as well. It is not the replacement but the enhanced version of cloud which provides a security on the cloud environment by isolating user's data which is saved on the Edge Devices. Fog Computing enables a user to save their data to nearby devices. In this paper the security issues also the technology which is used for security in this enhanced concept of cloud is mentioned.

1. Introduction

Cloud Computing is accomplishing fame and picking up consideration in business associations. It offers an assortment of administrations to the clients. It is a universal, advantageous; on request arrange access to a mutual pool of configurable registering assets due this straightforwardness, programming organizations and different offices are moving more towards cloud computing condition. To accomplish better operational proficiency in numerous associations what's more, little or medium organizations is utilizing Cloud condition for dealing with their information. Cloud Computing is a blend of a number of processing systems and ideas, virtualization and other which depend on the Internet. It is considered as a conveyance stage in which assets are given as a support of the customer through the Internet. In spite of the fact that, Cloud Computing gives a simple route for a overseeing and calculation of client information, however It likewise has some serious security dangers. There are a few conventional security components, for example, character, approval etc.As it is known that Fog Computing is present in the earth's atmosphere but Cloud Computing refers to the server which is situated at a far distance to which the large number of data can be stored and by the authentication a user can access the appropriate data from the server. Fog Computing is like the same as cloud computing but as every new technology which is introduced have a special feature in it like this Fog Computing has the same. By using this technology an user need not to save their data on a

distance server but to store the data on a nearby routers can be said as a Edge Device- the device by which an user can enter into the internet or can be said as it is the entry point into service provider core network example routers, phone, variety of Metropolitans Area Network (MAN) and WAN (Wide Area Network) also. It also needs not to use authentication again and again to use the appropriate data and an user can access the data more efficiently and faster because they have their devices which is more secure said to be themselves.

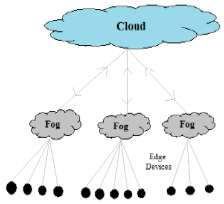


Figure: - Fog Computing

By using this technology Internet of things can also be used easily and efficiently. Internet of things is justifies by as Fog Computing is using different Edge devices in which three datasets of different types are considered and applied the analyzed encryption technique over those datasets. On validation, entire data over datasets is being accurately encrypted and decrypted back as well. We took android mobile as an edge device and deployed the encryption over datasets into it, so for easily communication and connection between these different devices for the data stored and retrieving within a network it can increase the security level of the data and its information contained because security is must for everyone now days. But by this way one drawbacks also came in between like if a third party access the user's routers in between the retrieving the data they can also use the same data. So, basically it can be said that Fog Computing is simply a concept by which data can be store in nearby devices not on the cloud computing which is a distance server. Fog Computing provides Quality of service and also reduces latency. In fog computing the users will be notified what are the actions that are needed to be taken on the data and then analytics are applied on the received data and stored it into the cloud. In the fog computing process application comes to the data not the data to the applications.

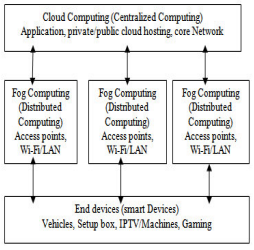


Figure: - Block diagram of reference architecture.

This computing gives Low inactivity and area mindfulness; it has Wide-spread topographical appropriation, underpins Mobility, and is bargained because of the enormous number of hubs. The principle assignment of haze is to convey information and place it nearer to the client who is situated at an area which at the edge of the system. Here the term edge alludes to various hubs to which the end client is associated and it is likewise called edge figuring. In the event that we look as per engineering haze is arranged beneath the cloud at the ground level. The term Fog computing is given by CISCO as another innovation in which cell phones interface with each other and bolster the information correspondence inside the Internet of Things.

At display each of the airplanes delivers around 20 terabytes of information created in a hour and they should be put away into cloud space. This is done to every one of the planes the world over

where recovering important information from cloud won't be conceivable driving for the need of haze processing. Cisco predicts that in the following decade, Internet of Things will be at 14.4$ trillion estimation of stake for organizations and Security in Fog Computing through Encryption enterprises. Web of Things had driven advancement to the fog computing in view of the expanded number of gadgets creating enormous measure of information.

Characteristics of fog computing:-

1. Edge area, area mindfulness and low inertness: Fog gives these qualities as in gaming, video spilling, and in enlarged realty.
2. Geological circulation: Cloud is concentrated in nature yet haze is appropriated topographically. So it assumes dynamic part in conveyance of fantastic information.
3. Haze underpins expansive scale sensor systems to screen the earth.
4. Large number of hubs, as outcomes of the wide geodistribution.
5. Support for versatility: Fog bolsters the applications to discuss specifically with cell phones so it underpins portability method.
6. Continuous communication: Fog gives ongoing association as opposed to group handling.
7. Heterogeneity: Fog processing is heterogeneous in nature and bolster assortment of situations.

2. Security of Cloud with Fog Computing:-

Various recommendations for cloud -based administrations portray strategies to store reports, records, and media in a remote benefit that might be gotten to wherever a client may associate with the Internet. An especially vexing issue before such administrations are extensively acknowledged concerns ensures for securing a users information in a way where that ensures just the client what's more, nobody else can access that information. The issue of giving security of classified data remains a center security issue that, to date, has not given the levels of affirmation a great many people want. Numerous recommendations have been made to secure remote information in the Cloud utilizing encryption and standard access controls.

Most would agree the greater part of the standard methodologies have been shown to bomb now and again for an assortment of reasons, including insider assaults, mis-arranged administrations, flawed executions, surrey code, and the innovative development of successful and advanced assaults not imagined by the implementer of security techniques. Building a dependable distributed computing condition isn't sufficient, on the grounds that mishaps proceed to happen, and when they do, and data gets lost, there is no real way to get it back. One needs to get ready for such mischance. The essential thought is that we can constrain the harm of stolen information in the event that we diminish the estimation of that stolen data to the aggressor. We can accomplish this through preventive‟ disinformation assault. We place that protected Cloud administrations can be executed given two extra security highlights:

1. User Behavior Profiling:

It is relied upon that entrance to a user’ s data in the Cloud will display typical methods for get to. Client profiling is an outstanding system that can be connected here to demonstrate how, when, and how much a client gets to their data in the Cloud. Such ordinary user‟ conduct can be ceaselessly checked to decide if irregular access to a client's data is happening. This technique for conduct based security is usually utilized as a part of extortion identification applications. Such profiles would normally incorporate volumetric data, what number of reports are ordinarily perused and how

frequently. These basic client particular highlights can serve to distinguish unusual Cloud get to construct in part upon the scale and extent of information exchanged.

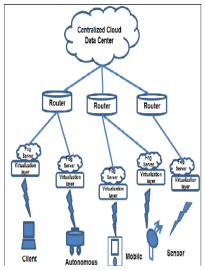


Figure: - Cloud Computing with Fog Computing.

2. Distractions:

Distraction data, for example, imitation archives, honey pots, and different counterfeit data can be produced on request and fill in as a methods for recognizing unapproved access to data and to poison" the thief's ex-filtrated data. Serving distractions will perplex and confound an enemy into trusting they have ex-filtrated valuable data, when they have not. This innovation might be incorporated with client conduct profiling innovation to secure a Client's data in the Cloud. At whatever point anomalous access to a cloud benefit is seen, bait data might be returned by the Cloud and conveyed so as to show up totally real and typical. The genuine client, who is the proprietor of the data, would promptly recognize when bait data is being returned by the Cloud, and subsequently could modify the Clouds reactions through an assortment of means, for example, challenge questions, to illuminate the Cloud security framework that it has mistakenly identified an unapproved get to The distractions, at that point, fill two needs:

(A) Validating whether information get to is approved when irregular data get to is distinguished.

(B) Confusing the assailant with counterfeit data. We set that the mix of these two security highlights will give extraordinary levels of security to the Cloud. No present Cloud security component is accessible that gives this level of security. We have connected these ideas to distinguish ill-conceived information access to information put away on a nearby record framework by impostors, i.e. aggressors who imitate honest to goodness clients subsequent to taking their qualifications. One may consider ill-conceived access to Cloud information by a rebel insider as the pernicious demonstration of masquerader. Our test brings about a nearby document framework.

3. Algorithm for Computing:-

1. Execute the identified operations.
2. Behavior of the user will be track by the profile including the following parameters:-
   - Username
   - Password
   - User key specified during document access
   - Type of document selected for access (valid or decoy).
3. After login the user login id and password is tracked and recorded or stored in database.
4. During document access, the user key specified is tracked along with the type of operation(valid or invalid)
5. Classify profile as valid or invalid using the following analyzed using the following mathematical operation: P(IV)=count(invalid operations of each type)/count(operations of each type).

6. If the value P(IV) is above a threshold parameter then the profile is categorized as invalid and the user is redirected to the decoy module.
7. If access of third part is login in between then lost the connection of the devices in between.
8. A login password key is generated to the main user with a warning to change its password for the access.
9. And if third party downloads or retrieves data then a key generate with a message and stored in the data base.

4. Security Techniques Applied:-

Data Encryption standard (DES) was once most broadly utilized encryption standard, which utilizes symmetric key calculation for encryption of information. This was thought to be fundamental building obstruct for the progression in the cutting edge cryptography in exhibit world. DES has 56 bits of key size and though the square size is 64 bit. For some applications when considered DES is said to be the most uncertain strategy for some applications. This is a result of its key size which is 56 bits and this could be beast constrained. Two organizations together had softened the DES calculation key up 22 hours and 12 minutes. This shows how frail the calculation is. A portion of the assaults that could break the key quicker than the Brute power are Differential Cryptanalysis, Linear Cryptanalysis and Improved Davies Attack. The ancestor of the DES calculation is 3 DES which is named as Triple Data Encryption Standard. Where 3 occurrences of DES are fell. The underlying 56 bit key was adequate, however the expansion in computational control made beast compel simple. Triple DES has rolled out no improvements to the past DES calculation aside from the expansion in the key size, where it can have 56 or 112 or 168 bits of key size and though the piece measure stays same as 64 bits as DES. Triple DES was said to be 2½ time more secured than the DES calculation. Indeed, even in Triple DES is powerless against security assaults meet in the center assault.

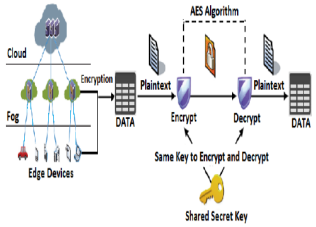


Figure: - Working of Encryption technology in fog computing.

As DES calculation was intended for equipment usage, it isn't solid in equipment similarly Triple DES don't work legitimately in programming applications. To defeat the above issue said Advanced Encryption Standard (AES) is considered as more powerful. Which is thought to be the most advanced? Furthermore, secured standard for encryption of electronic information. AES is thought to be successor of the DES which utilizes standard symmetric key encryption for a large number of the US government associations. AES acknowledges of the key size of 128, 192, 256 bits of size. While 128 is as of now thought to be unbreakable and there were many open rivalry held by numerous association to break the key however it was never done. On contrasting all the accessible encryption calculations, AES would be the better and most secured sort of calculation that could be executed in the haze. So far encryption procedure has not been proposed for security in the haze registering. As a conclusion over all the distinctive sort of encryption strategies, AES can be considered more appropriate and versatile for nature of mist.

5. Proposal for the future work:-

These days enormous measure of information is put away on cloud. Cloud registering guarantees to altogether change the way we utilize PCs and access and store our own and business information. Because of these new figuring and correspondence worldview there emerge information security challenges. At the point when unapproved get to be distinguished that client's action will be followed. In view of the exercises performed by unapproved client administrator can close the association in the middle. At the point when another client goes into this System, he need to enroll first. Furthermore, after this, whatever activity he is doing that additionally will be spared in the database. In each case it now will execute client conduct calculation. in the event that the outsider access the switches in the middle of the correspondence the client got a popup message to change the secret word and the movement done in the middle of the correspondence by the outsider is spared and that can be seen by the client and after that client can adjust or refresh the information as their own view.
It results to the security level of the data and information of the user over the network within the devices.

6. Conclusion:-

With the expansion of information burglary assaults the security of client information security is turning into a difficult issue for cloud specialist co-ops for which Fog Computing is a worldview which helps in checking the conduct of the client and giving security to the client information. Haze Computing presents another approach for tackling the issue of insider information burglary assaults in a cloud utilizing progressively created distraction documents and furthermore sparing capacity required for keeping up fake records in the cloud. So by utilizing fake method in Fog can limit insider assaults in cloud.

Reference:-

[1]Clinton Dsouza Gail-Joon Ahn Marthony Taguinod,"Policy-Driven Security Management for Fog Computing:PreliminaryFrameworkandACaseStudy," Laboratory of Security Engineering for Future Computing (SEFCOM) School of Computing, Informatics, and Decision Systems Engineering Arizona State University.IEEE IRI 2014, August 13-15, 2014.

[2]Ryoichi Sasakiand Tetsutaro Uehara,Fog Computing: Issues and Challenges in Security and Forensics, Cambridge University Press, Cambridge, 1982. 0730-3157/15© 2015 IEEE.

[3]Cloud SecurityAlliance, "Top Threat to Cloud Computing V1.0," March 2010.[Online].

[4]M. Ben-Salem and S. J. Stolfo, "Modeling user search-behavior for masquerade detection," in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.

[5]M. Arrington, "In our inbox: Hundreds of confidential ltwitter documents," July 2009. [Online].

[6]William Y Chang, Hosame Abu-amara, Jessica Stanford,"Transforming enterprise cloud services".

[7] Marinos A. & Briscoe G., Community Cloud Computing (pp. 472-484). Heidelberg: Springer, 2009,pp. 472-484.