International Journal of Engineering & Technology, 7 (2.8) (2018) 680-683

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

An efficient fog computing for comprising approach to avoid data theft attack

T. Pavan Kumar, B. Eswar, P. Ayyappa Reddy*, D. Sindhu Bhargavi

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, Andhra Pradesh, India-522502.
**Corresponding author E-mail: eswarbalisetty44@gmail.com*

Abstract

Cloud computing has become a new paradigm shift in the IT world because of its revolutionary model of computing. It provides flexibility, scalability, and reliability and decreased operational and support expenses for an organization. The Enterprise edition software's are very costly and maintaining a separate IT team and maintaining their own servers is very expensive and that's the reason why most of the companies are opting for Cloud computing over enterprise edition of the software. However, few organization cloud customers are not willing to step to cloud computing up on a big scale because of the safety problems present in cloud computing. One more disadvantage of Cloud is it's not suitable for another revolutionary technology i.e. IoT (Internet of things)

In this paper we are going to present the Advantages of Fog Computing and Decoy technology to address the security in cloud computing by extending it into fog computing.

Fog Computing is a new paradigm in which the computing power moves to the edge of the network. So, it's also called as Edge Computing.

Keywords: *Edge Computing, Decoy Technology, Data Integration and Security Issues Verification.*

I. Introduction

Edge computing is accomplishing prominence and picking up consideration in business associations. It offers an assortment of administrations to the clients. It is a widely spreading throughout an area to organize and to access to a pool which is mutual for configurable registering action. Due this simplicity, programming organizations little and medium organizations (SMBs), are progressively settling on outsourcing information and calculation to the Cloud. This clearly bolsters better operational proficiency, however accompanies more serious dangers, maybe the most genuine of which are information burglary assaults. Information burglary assaults are determined to be the best dangers may occur to the distributed computing over the Cloud Security. Even though the aggressor is more associate than the odds of information burglary increment as the associate may contain some individual data. So, regular thought of a cloud associate as a maverick manager of a specialist organization is spoked about, however we likewise display two extra cloud-related associate chances: the associate who misuses a cloud related helplessness to take data from the cloud framework, and an associate those utilizes cloud frameworks to do an assault in a business neighbourhood asset. Mist Computing is an expansion of Cloud Computing. Most research in Cloud figuring that the safety has concentrated on methods for counteracting unapproved and ill-conceived log-in to the data by creating refined log-in control and encryption systems. However, these components have not possessed the capacity to forestall information trade off. We propose a totally unique way to deal with securing the cloud utilizing imitation data innovation, so we may have to come to call the Edge Computing. Let us take Edge computing as a worldview where we can give neighbourhood ingress to the client and with the assistance of fake innovation, we give defence to client information and forestall insider robbery assaults.

1.1 Need for Fog Computing

Although Cloud computing has provided solutions to most of the problems faced by organizations. It's not suitable for IOT because in IOT faster access of the data, processing and transmitting of data is needed. Cloud cannot provide these necessary things as its far from the device (IoT device). The solution for this is Fog/Edge computing. The Fog is named as a metaphor to cloud as Fog is nothing but Cloud near to land. Similarly, in Fog computing the computing and processing power is moved near to the device (IoT device). Let's consider two scenarios where Fog computing is necessary for IoT.

2. Exiting System

Edge computing is a strategy which gives administrations to customer over the system; client can utilize any sort of administrations (Software as a Service, Platform as a Service, and Infrastructure as a Service). Distributed depository is the design of system venture stockpiling where tremendous measure of information is put away. Edge computing gives depository room administrations to the clients, client can put away his information and data inside the cloud and he may ingress to data as contain it frame any PC associated with the internet. The primary concern is that the client doesn't know where and how information is put away? and who can see the information? The issue of client when he stores touchy data in the cloud the client requires security of the distributed computing to confirmation no one can appropriate to utilize and see his information and business-related data that his store in cloud, to evade this issue utilized encryption method. But encryption technique unsuccessful in anticipating information burglary assaults. By applying encryption method to the data, we can't acknowledge add up to assurance to private information. In Existing framework according to the survey done it is watch that creating distraction document is done at whatever point updated record is being transfer to the cloud was proposed however in that case require immense measure of depository room in the cloud.

Disadvantage

1. No one knows when the assault is happened.
2. It is perplexing to recognize which client is assault.
3. We can't identify which document is hacking.

3. Proposed System

Here we get an alternate way for making information more secure in the cloud utilizing hostile fake innovation. The information burglary by associate is basically passed with the assistance of making of distraction document on request. we verify the information entry on cloud to recognize unusual data entered to designs. At that instance when unlawful login is assumed and there after confirmed by using the critical problems, we send misinformation hit by getting a lot of distraction matter to the aggressor. In the framework we create at whatever point insider saw to perform information burglary, at exactly that point distraction record is made and is passed on to the asking for insider, at whatever point client attempting to transfer a document on the cloud client give security question. Similar security questions shows up when any client need to download or to do the operation perform on the specific record shape the cloud. In case associate tries to download a similar record indeed the utilization of time stamp-based key gives him another fake document when contrasted with the past which will confound him. This ensures against the abuse of the user's genuine information. Here we will provide a One Time Password framework at the client level in this framework. The One Time Password framework may create a check code where the client need to place amid enlistment. There after the code will be affirmed by the Third-Party Administrator and simply after his approval the client enlistment will be finished. Next moves to the transferring and downloading of documents. While transferring the imaginative information will be sent to the Cryptographic Service Provider and a duplicate of it is sent to the Third-Party Administrator for validation. After a basic yes/no message from the Third- Party Administrator the creative record will be prepared further for division and encryption by the Cryptographic Service Provider. This will likewise lessen the overhead essentially. The rights to adjust refresh or erase will just exist in with the proprietor of the information along these lines guaranteeing a most select level of Security. Inside the Data Base administrator is additionally observed by the Third-Party Administrator with a specific end goal to keep a beware of any type of mischievous movement. Information lost can likewise adequately recover utilizing standby servers RAID LEVEL-1. Other determinations in the application incorporate computerized marks.

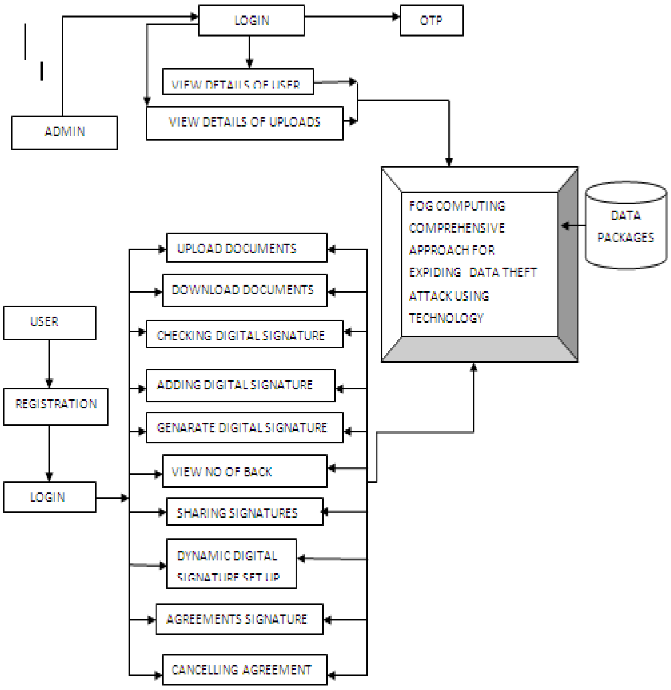

Fig.1: System Architecture

4. Securing Clouds

The basic thing is to limit the danger of stealing the data if we reduce the prediction of that thieve data to the hacker. One can achieve it through a, preventive misinformation strike. We envision that protected Cloud administrations can be actualized given two other security highlights.

A. Mistaking the trigger person for shame information

We envision that the mix of these two security highlights will give unmatched levels of securities to the Cloud. No present Cloud security strategy is accessible that gives this level of securities. People have helpful for ideas to see illicit information access to information put away on a neighbourhood record framework by impostors, i.e. assailants who duplicate legitimate clients after robbery their distinguishing proof. One may consider unlawful access to Cloud information by a scoundrel associate as the vindictive demonstration of an impostor. Our trial brings about a nearby document framework setting demonstrate that consolidating the two strategies can yield better acknowledgment comes about, and our outcomes prompt the way which might work in a domain of cloud. As the proposed statement on cloud is as clear for the client as a neighbourhood record framework. In the accompanying we investigation quickly a portion of the trial comes about accomplished by utilizing this way to deal with identify disguise movement in a neighbourhood record setting.

B. Module Description

1) User Profiling
2) Decoy reports
3) Secure from merchant
4) Block the terrible client
5) Differentiate client

1) Customer profiling conduct method: Here the administrator will have record of all clients with the goal that he can without much of a stretch set working gauge for lawful client. Administrator screen information access in the cloud and notice anomalous information get to design User profiling will an outstanding Technique that can be available here to check and how much a customer gets his information in the Cloud Platform. That kind of difficulty behaviour can be constantly verified to decide for anomalous access to customer information is understanding. This strategy is based upon the security will routinely use as a part of plan revealing enquiry. Such profiles would clearly unprofessional data, whether available records are generally reused and how regularly. We check for anomalous pursuit practices that show deviations from the client pattern the association of hunt activities distinction distinguishing proof with trap-based bait documents ought to give more grounded affirmation of misbehaviour, and in this manner, recuperate an identifier's precision.

2) Decoy archives module: We recommend an alternate approach for securing information in the cloud utilizing frightful bait innovation. We screen information control on the cloud and sense unpredictable data carry to designs. We start a misinformation hit by repeating a lot of bait information to the attacker. It secures upon the misuse of the customers genuine information. We utilize this innovation to start disinformation assaults against malignant insiders, keeping them from recognizing the legitimate mindful client information from sham futile.

3) Secure from merchant: If legal customer didn't have any wish to provide entry for the merchant so we will ensure that entrance frame dealer. Over the past framework, dealer may straight acquire to the possess or national level data which is away from the fog. No other is available for the circumstance for the security of data which kept apart in to the cloud/fog. So, in our arranged framework, individual information which kept apart on the cloud is kept, it is absolutely rely upon the client to dole out permission concurrence for its information. If merchant need to get to the data which is kept apart in the cloud, which helps to take the private key for that specific customer to decrypt the data and these strategy is get completed by means of safe key supplant calculation.

4) Block the dreadful client: If the client is terrible then his profile straight obstructs that client. Client progressively bombs in access, creature look attacks, upload records which contains .exe documents with in it and so on along these lines, All this record of the all client will kept up in the client profiling exercises, so when framework distinguishes any frightful exercises, it specifically obstruct that client in the event that, if any permitted client endeavour to look through some other broadly put away records at that point as per our circumstance our framework hinders that customer, yet amid blocking framework asks security inquiries to that client to stay away from acknowledged client sticking.

5) Differentiate client: The rights of client can be separated by utilising his contacts. One can assign rights of human at the season of transferring. At an instance low client have just perused consents, high client has all authorizations like adjustment. By classifying diverse clients on the cloud, we get reasonable and adaptable control over seeing assets upon the cloud.

5. Surveillance Camera

Let us consider the working of a surveillance camera in a street or a shopping mall. The camera records everything and it will send the whole recorded data to the cloud. Inside the Cloud the server processes frames and removes the static (no motion in frame) frames and records the frames that have motion. The disadvantage with this approach is

1. Over Utilization of Network Bandwidth
2. It takes more time to get the results because the data has to make round trip

Let us consider another serious scenario where the cloud computing approach will cause catastrophic failures

5.1 Driver Less Cars (IoT Application1)

Driver less cars, Automated Parking cars are gaining huge popularity and one of the best IoT Application.
Let's suppose a Driver less car is running on the road and it has a sensor that detects objects and sends the details about the object to the Cloud and the Cloud server must give instruction to the car whether to apply brakes, or go sideways, or hit it if it's an object like paper or cloth etc. The time taken would be
Time taken = Time to transmit data from Car to Cloud server + Processing the data in Cloud Server +Time to transmit the instruction from Cloud server to Car.
By the time the instruction reaches the Car anything may happen. Hence the traditional Cloud computing approach will not work for IoT Applications, so we move to a more powerful technology which extends the cloud called as Fog which will be near to the nodes

5.2 Solution To Above Problems by Fog Computing

The solution to above scenarios using Fog Computing.

1. The Fog node near the surveillance camera will remove the static frames and send only the non-static frames to the cloud there by saving lot of Network- Bandwidth and It can also act by processing the non-static frames if there is any malicious activity. After processing the Fog node will send the data to Cloud for long term analysis
2. In case of Driver less cars the Fog nodes are placed separately from each other with some distance. The Fog node will process the object data and give instruction to the Car. As it's near to the Car the instruction will be in time without any latency.
   We can make inference from the above two scenarios that

1. The application's which have time sensitive data should be equipped with Fog nodes. The time sensitive data should be processed by the Fog node and later it will send the data to Cloud for long term analysis.
2. Network-Bandwidth will be saved with the use of Fog Computing

Note: Fog Node will have limited processing and storage capacity compared to Cloud server. The Fog Computing will not replace or make Cloud computing obsolete It acts as an extension to the cloud computing. As Fog is inherited from Cloud. The problems that are existing in the Cloud also prevail in Fog Computing. The main issue among them is Security. For this we propose a new technology in Security called as Decoy Technology.

6. Conclusion

We actualized an alternate way of securing individual and business information within cloud/fog. People suggest a framework to avoid information get to patterns by profiling client conduct to build up when an underhanded insider criminally gets to somebody records in the cloud administrations. The bait innovation enables the utilization to keep imitation data or sham data in the document framework to misdirect insider information robbery assailants. We might want to expand the client profile administration and utilize more bait data from different spaces for enlightening careful positives of the haze registering.

References

[1] 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.

[2] “Protect Sensitive Data in Public Cloud from a Theft Attack anddetectAbnormalClientBehaviour”May2014http://ijesc.org/upload/cb5bd9241011e5817686fbf01bfe503e.Protect%20Sensitive%20Data%20in%20Public%20Cloud%20from%20an%20Theft%20Attack%20and%20detect%20Abnormal%20Client% 20Behavior.pdf

[3] Cloud Security Using Fog Computing Proceedings of IRF International Conference, 30th March-2014 http://iraj.in/up_proc/pdf/56-13963354905-7.pdf

[4] V. Sriharsha Student, Dept. Of CSE SNIST, Ghatkesar, India V. Prabhakar Dept. Of CSE. SNIST, Ghatkesar, India N.Krishna Chythanya SVSIT, Warangal, India “Dynamic Decoy File Usage to Protect from malicious insider for data on public cloud” International Journal of Advanced Engineering and Global Technology Vol-1, Issue-3, October 2013 http://ijaegt.com/wpcontent/uploads/2013/10/IJAEGT-309128-page-98-102.pdf

[5] Securing the cloud using Decoy Information Technology to prevent them from distinguishing the Real Sensitive data from fake Worthless data Etikala Aruna, Dr. Ch GVN Prasad, A. Malla Reddy Issue9,September2013http://www.ijarcsse.com/docs/papers/Volume_3/9_September2013/V3I 9-0155.pdf

[6] Minimizing Internal Data Theft in Cloud Through Disinformation Attacks P. Jyothi1, R. Anuradha2, Dr.Y. Vijayalata3 International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September2013http://www.ijarcce.com/upload/2013/september/20Jyothi%20P%20Minimizing%20Internal%20Data%20Theft%20in%20Cloud.pdf

[7] Secured Cloud Computing With Decoy Documents 1dnyanesh S. Patil, 2suyash S. Patil, 3deepak P. Pote, 4nilesh V. Koli Proceedings of 4th IRF International Conference, Pune, 16th March-2014 http://iraj.in/up_proc/pdf/52-1395229730159-161.pdf

[8] Madhusri.K,Navneet. “Fog Computing: Detecting Malicious Attacks in a cloud international Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[9] Cloud Security Alliance, “Top Threat to Cloud Computing V1.0,” March 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[10] M. Arrington, “In our inbox: Hundreds of con- fidential twitter documents,” July 2009. [Online]. Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-ofconfidential-twitter-documents/

[11] D. Takahashi, “French hacker who leaked Twitter doc- uments to TechCrunch is busted,” March 2010. [On- line]. Available: http://venturebeat.com/2010/03/24/french-hacker-who- leaked-twitter documents-to-TechCrunch-is-busted/

[12] D. Danchev, “ZDNET: French hacker gains access to twitter’s admin panel,” April 2009. [Online]. Avail- able: http://www.zdnet.com/blog/security/french-hacker-gains-access-totwitters-admin-panel/3292 [13] P. Allen, “Obama’s Twitter password revealed after French hacker ar- rested for breaking into U.S. president’s account,” March 2010. Available: http.

[13] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T “Review and Analysis of Promising Technologies with Respect to fifth Generation Networks”, 2014 First International Conference on Networks & Soft Computing, ISSN:978-1-4799-3486-7/14,pp.270-273,August2014.

[14] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.

[15] P Bala Gopal, K Hari Kishore, B.Praveen Kittu “An FPGA Implementation of On Chip UART Testing with BIST Techniques”, International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 14 , pp. 34047-34051, August 2015.

[16] Murali, K Hari Kishore, D Venkat Reddy "Integrating FPGAs with Trigger Circuitry Core System Insertions for Observability in Debugging Process” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.11, Issue No.12, page: 2643-2650, December 2016.

[17] Mahesh Mudavath, K Hari Kishore, D Venkat Reddy "Design of CMOS RF Front-End of Low Noise Amplifier for LTE System Applications Integrating FPGAs” Asian Journal of Information Technology, ISSN No: 1682-3915, Vol No.15, Issue No.20, page: 4040-4047, December 2016.

[18] N Bala Dastagiri, K Hari Kishore "Novel Design of Low Power Latch Comparator in 45nm for Cardiac Signal Monitoring”, International Journal of Control Theory and Applications, ISSN No: 0974-5572, Vol No.9, Issue No.49, page: 117-123, May 2016.

[19] N Bala Gopal, Kakarla Hari Kishore "Reduction of Kickback Noise in Latched Comparators for Cardiac IMDs” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.43, Page: 1-6, November 2016.

[20] S Nazeer Hussain, K Hari Kishore "Computational Optimization of Placement and Routing using Genetic Algorithm” Indian Journal of Science and Technology, ISSN No: 0974-6846, Vol No.9, Issue No.47, page: 1-4, December 2016.

[21] N.Prathima, K.Hari Kishore, “Design of a Low Power and High Performance Digital Multiplier Using a Novel 8T Adder”, International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 3, Issue.1, Jan-Feb., 2013.

[22] Meka Bharadwaj, Hari Kishore "Enhanced Launch-Off-Capture Testing Using BIST Designs” Journal of Engineering and Applied Sciences, ISSN No: 1816-949X, Vol No.12, Issue No.3, page: 636-643, April 2017.