International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Fog Computing : Implementation of Security and Privacy to Comprehensive Approach for Avoiding Knowledge Thieving Attack Exploitation Decoy Technology

Geetha Kurikala[1], K Gurnadha Gupta[2],A.Swapna[3]
[1,2]Assistant Professor, Department of Computer Science and Engineering, Sri Indu College of Engineering & Technology, Telangana, India
[3]Assistant Professor, Department of Information and Technology, Sri Indu College of Engineering & Technology, Telangana, India

ABSTRACT

Now days, Cloud network is less secure or defend the data on cloud from the data felony attacks, principally corporate executive attacks. An oversized and secure of skilled and private information is kept on Cloud server. Cloud network storage is getting used in numerous industrial sectors. During this sector of the abundant blessings of storing information on cloud, Security still remains a serious downside that must be conquered. Computers system is employed to access the data on Cloud, with the new communication and computing network produce new information security challenges. The subsisting ways of protective secure and vital information on cloud have unsuccessful in preventing information felony attacks. AN altered approach is administrated for securing the data, additionally to the previous normal cryptography mechanisms. The user's victimization the Cloud square measure monitored and their access patterns square measure recorded. All Users have a novel profile that is monitored and updated to the server. Once AN unwanted activity like unauthorized permission access or random and untargeted hunt for information is detected that isn't seemingly to be of the $64000 user, a misinformation attack is launched. The any user or one who is attempting to access the own information is formed to answer the protection queries. An oversized quantity of Decoy information is provided or out there to the aggressor that successively protects the user's real information.

Keywords: Cloud Computing, User Behavior Profiling, information Security and truth proof, Fog Computing, Security.

I. INTRODUCTION

Fog computing may be a term generated by Cisco refers to increasing cloud computing to the enterprise's edge network. In addition referred to as fogging or Edge Computing, fog computing provides the accomplishment of storage, calculate and networking service between cloud computing knowledge centers and end services. Cisco planned its fog computing vision in Jan 2014 as a way of transfer cloud computing skills to the top begin and as a result, nearer to the oftentimes increasing no. of interconnected applications and devices that consumes cloud adoption and manufactures additional and larger amounts of information. By handling these services build up the online of things (IoT) at the sting of the network, knowledge match basically in several things be of methodic lots of effectively than if it required being forwarded to the cloud for process. The thought} behind broadcasting knowledge to network advancement is that the construct of fog computing and this has been created gettable by CISCO iox platform. Open offer code Linux and CISCO ios network software unit combined to form the design of iox. 2 software for communication and computation in Cisco routers. The Communication and computing declare for internet of things has been provided by one platform spoken as iox. Linux transforms routers to mini-computer by that we have a tendency to tend to groundwork run third party application. The Cisco iox permits users to assembly their OS and application in its open and extensible surroundings. The budget we are going to develop our own wise application to use

the power of fog computing. The iox platform provides associate SDK and middleware coupling by that we have a tendency to tend to depths diet attract, interface and analyze knowledge domestically in real world. It the appropriateness to concisely inactive and takes users concern spat inside the grinding appliance upon to the span do knowledge for immediate action. It consumes minor time by ally your application with any protocol, device or interface. Iox platform analyzes knowledge in real time. The open application surroundings advocate lots of developers to bring their property interface and own applications at the network edge. Fog computing offers knowledge, storage, compute, and application facilities to end-subscribers. The distinctive Giveaway look is its look to end-subscribers; it's shelved for quality and its dense geographical oversight. Coupling unit hosted at the sting of a network or even end devices i.e. admission in purpose of reality and set-top-boxes. By attainment consequently, Efface decreases facilitate latency, and enhances associated with of Services (QoS), resulting in best subscriber-experience. Fogginess Computing provides suspended to evolution internet of Fullness (IoE) applications saunter needs unqualified-time/predictable latency (industrial automation, transportation, networks of actuators and sensors). Gratitude to its adequate geographical distribution the Fogginess exemplary is essentially set for real time analytics and real time large data. Fog provides support to impenetrable distributed data points, thus the adding the fourth axis to the in any respect times acknowledged specified large data dimensions. the required decrement in data effort in data movement throughout the network shriveled price and latency, blockage, price and removal of bottlenecks succeeding from centralized computing systems, inflated security of encrypted observations as a result of it remains nearer to the eradicate subscriber decreasing exposure to hostile components and inflated measurability raising from virtualized systems. Designate the shabby computing feeling; suitably diminish associate objective of failure and a significant block. Can increase the protection, as knowledge area unit understood because it is simulated favor the dominance of network. Superiority Computing, AN auxiliary to largesse sub-second recognition to finish subscribers, it in addition to offers forward levels of counting on, measurability and fault tolerance and Consumes low band breadth.

FOG computing bridges the gap between statistics centers operating in a normal Imperceptive computing design, and finish points. Extent production, as a result, it in addition to provides for a receive, take counsel there, waste gritty integral and a cautious result that accords process power, storage, and network service. During this accessible of divide, applications And cohort figures process occur at the unambiguous profit or bounds of the network in an Obtunding computing setting. The observations process and order of the applications aren't for much longer focused inside the Cloud. In administration, therefore, Dim Computing brings applications and knowledge nearer to end-users. This is often the main focus of Dim Computing. Link of the fundamental technologies worn to depute Mask Computing is that the renounce. A depart from could be a microcontroller that comes relative to its react to constitutional retention, associate interface for knowledge persist, and gift feeling Mesh chip bundled on in concert unit. A drop is steaming by a dense aggression that inside the ultimate persists sure a span of years. User's unit nonconformist to affix plebs' trade-mark of sensors which could discover temperature, light, and voltage. Fogginess Computing is layered not up to Cloud associate degreed acts as AN exit that permits improvement of transfer of information and services. The array of Fuzz Computing in affinity with Cloud is shown inside the escort Figure 1.

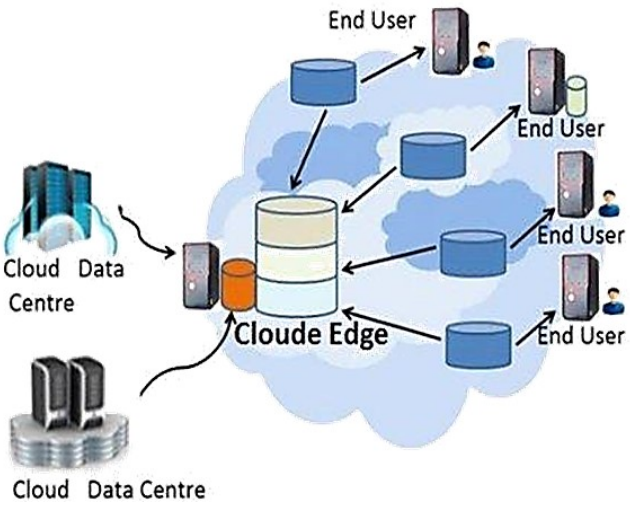

Figure 1. Fog Computing

II. METHODS AND MATERIAL

Cloud computing means that sharing of computing resources throughout any communication network by

using virtualization. Virtualization permits a server to be sliced in virtual machines. Each virtual machine has its own applications/operating system that quickly regulate resource distribution. Cloud computing provides many blessings; one amongst them is versatile resource distribution. To satisfy the wants of clients, cloud environment ought to be elastic in nature and might be acquiring by effective resource allocation. Resource allocation is that the development of allocating existed resources to clients throughout the net and plays vital role in Infrastructure-as-a-Service (IaaS) model of cloud computing. Versatile resource allocation is required to optimize the assignment of resources, reducing the latent period and increasing the output to boost the cloud computing performance. Enough resolutions are introduced for cloud computing to boost the performance except for fog computing still effective solution ought to be discovered. Fog computing is that the virtualized treated layer between cloud and clients. It's an extremely virtualized technique that is same as cloud and supply computation, data, storage, and networking facilities between cloud servers and finish users. This paper presents a good algorithmic program and design for resources provisioning in fog computing environment by using virtualization technology.

A. LITERATURE SURVEY

The existing system is less secure to observe the unauthorized users and may be easily hacked by anyone skilled in hacking field. we tend to facility of security questions has been provided to the prevailing system then conjointly the obtainable system is incredibly poor system and fewer secure. Anyone United Nations agency possesses unauthorized access to cloud will explore for files and data. The system isn't ready to establish whether or not the user is legitimate or not. If the person is permitted and illegitimate then conjointly this method sends the initial data to the user. So existing system isn't secure. Encryption methodology is provided to existing system however cloud server and valid data isn't secure by solely encryption.

"Fog Computing: Mitigating business executive data thieving Attacks within the Cloud", this paper explains monitor data and provides data security from unauthorized intruders and confusing the aggressor and unauthorized users concerning the $64000 data.

Advantages:
1-User Behavior Profiling
2-Decoy Information technology
"Software decoys for insider threat", during this paper author, discussed a method that confuses the business executive and attacker also used obfuscation that helps to secure data by concealing it and creating it decoy info for insider.

Advantages:
Developed a method that was a computer code decoy for securing cloud data.
"Reliability within the Provides 3 tier design Utility Computing Era: Towards Reliable Fog Computing", in this paper author suppliers feasibility to real time objects wherever the user will perform the operation on cloud computing.

Three tier designs for Fog Computing are used.
"Improving Websites Performance exploitation Edge Servers in Fog Computing Architecture", this paper provides varied methods area unit combined and used with the unique data to improve the performance of rendering an online page.
This projected system reducing the dimensions of net objects, minimizing and obstruction HTTP requests, and reorganizing the web page.

B. PROPOSED WORK

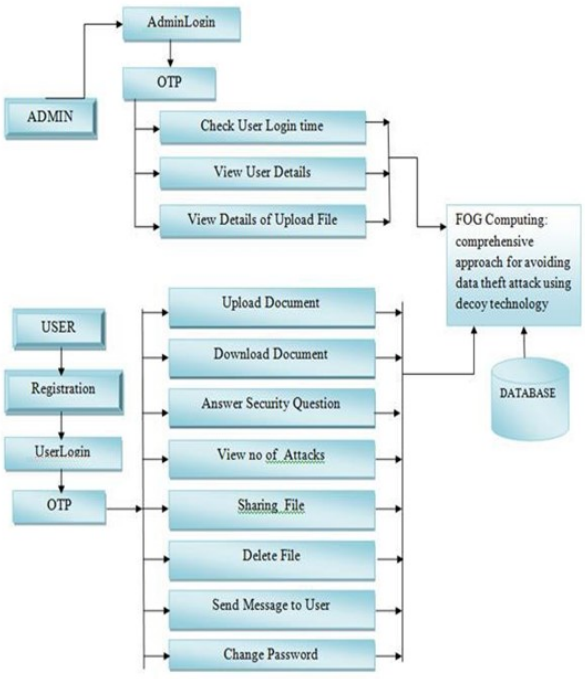

Figure 2. System architecture

Above fig. states the actual working of the fog computing .In two ways login is done in system that are admin login and user login .When admin login to the system there are again two steps to follow: step1:Enter username step2:Enter the password . After successful login of admin he can perform all admin interconnected works, but at the same time as downloading any folder from fog he have to answer the security Question if he answer it correctly then only original file can be download.

In other case, when admin or user answer incorrectly to the security question then decoy document (fake document) is provided to the fake user. Decoy technology work in the given manner if you have any word ,suppose "MADAM" in the document then some alphabets are replaced as M->A then the given word become "AADAA" which have no meaning. In some Case, if attacker getting to know that „M‟ is replaced by „A‟ in the given document and by applying reverse engineering he get result as "MMDMM". In any case he can't judge content of document. When client login to the method he also have to follow the same procedure as admin. Perform operation like share file upload documents, download files, view alerts, forward msg to another user, understand message, transmit any message all these can be perform by the user. prepared this flow provide the detail knowledge of attack done on their personal file/document with details like date, time, no of times the hacker trying to hack that file .Best thing of fog Computing is after each successful login the user get SMS on the mobile that „User login successful‟. starting this the user obtain alert when other else trying to gain access to his/her personal fog account and when attacker trying to download some files/documents then user also get SMS that contain attacker ip-addr, hacker's server name, time, date details on his/her mobile so that become easy to catch attacker by tracing all these effects. In this technique fog computing is extra protected than the conventional cloud computing.

We propose a completely different approach to securing the cloud using decoy info technology, that we've got come back to decision Fog computing. We have a tendency to implement the new technology to launch misinformation attacks against malicious insiders acting on the cloud, preventing them from distinctive the $64000 sensitive client data from faux tin-pot data. The system decoys, then, serve 2 purposes: (1) we have a tendency to check or confirmative whether or not data access is permitted once abnormal info access is detected, and (2) the second is confusing the attacker with fake info.

Module Description:

1. Cloud Computing.
2. User Behavior Profiling:
3. Decoy documents.

Cloud computing

Cloud computing could be a model for sanctioning convenient, on demand network access to a shared pool of configurable computing resources we have a tendency to take the instance, networks, servers, storage, applications, and services that may be space provisioned and free with bottom management effort or service-provider interaction. It divides into 3 kinds

1. Application as a service(AaS).
2. Infrastructure as a service(IaS).
3. Platform as a service(PaS).

Cloud computing exhibits the subsequent key characteristics:

1. We improve with users' ability to re-provision technological infrastructure resources.
2. We have a tendency to additionally price is claimed, reduced and in a very public cloud delivery model capital expenditure is converted to operational expenditure.
3. Virtualization technology permits servers and storage devices to be shared and utilization is raised. Applications are often simply migrated from one physical server to a different.
4. Multi resources access and prices across an outsized pool of users so permitting.
5. Centralization of infrastructure in locations with lower prices for inside of your time we will access resources (such as land, electricity, etc.)
6. We have a tendency to additionally analyzed the employment and potency enhancements for systems that square measure usually solely 10–two-hundredths utilized.
7. We have a tendency to additionally responsibility is improved if multiple redundant sites square measure used, that makes well-designed cloud computing appropriate for business continuity and disaster recovery.
8. Performance is monitored and consistent and loosely coupled architectures square measure made

victimization net services because of the system interface.

9. Security may improve thanks to the centralization of data, accrued security-focused resources, etc., however considerations will persist regarding loss of management over sure sensitive data and also the lack of security for keep kernels.
10. Maintenance of cloud computing applications is simpler as a result of they are doing not got to be installed on every user's pc and might be accessed from completely different places.

Client Behavior Profiling:

We check information access on the cloud and distinguish unusual information get to designs User conduct profiling strategies is a well best Technique that can be connected to the proposed framework display. This specialized investigation the how, when, and how much a client gets to their data in the Cloud server. Get to „normal user‟ conduct can be persistently checked to decide if irregular access to a user‟s data is happening. This strategy for conduct based security is utilized to distinguish the extortion identification applications framework. Such profiles would normally incorporate volumetric data, what number of archives are commonly perused and how frequently. We likewise screen for strange hunt practices that display deviations from the client pattern the checking right of inquiry conduct oddity location. When we utilize trap-based bait records ought to give more grounded prove verification of the aggressor, and hence enhance a detector‟s precision.

Decoy Documents:

We apply the various new approach for securing information of users within the cloud exploitation offensive decoy technology. we tend to data access within the analyze and monitor cloud and discover abnormal service data access patterns. We implement a misinformation attack by returning huge amounts of decoy data data to the aggressor. this system protects against the misuse of the user‟s from real data. We used new technology to launch misinformation attacks against malicious insiders, preventing them from distinguishing the important sensitive client data from faux worthless data the decoys, then, serve 2 purposes:

(1) we tend to confirming whether or not data access is allowed, person when abnormal data access is detected, and

(2) We tend to confusing to the aggressor with fake data

III. RESULTS AND DISCUSSION

IV.CONCLUSION

We reason that an examination, with the expansion of information burglary assaults on cloud, the security of client information is turning into a significant issue for cloud specialist co-ops for which our proposed framework haze figuring is a worldview which helps in checking the conduct of the client which action they perform and giving security to the client information. Different strategies talked about in this investigation paper utilize mist figuring for improving and breaking down the site execution issue. We finish that by proceeding with this proposed work utilizing Fog Computing stages can prompt exceptionally extremely solid systems and would contribute in expanding the level of security if client information on the cloud so the client has given greater security.

V. REFERENCES

[1]. Yogesh K Nath, Rupesh R Bhairat, Ajit N Ghagare" Implementation of Security and Privacyon Fog Computing using DecoyTechnique" International Engineering Research Journal (IERJ), Volume 2 Issue 9 Page 3446-3448, 2017 ISSN 2395-1621

[2]. D. C. Saste, P. V. Madhwai, N. B. Lokhande, V. N.Chothe, "FOG COMPUTING: Comprehensive Approach for Avoiding Data Theft Attack Using Decoy Technology", IJCTA, Sept-Oct 2014.

[3]. 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.

[4]. "Protect Sensitive Data in Public Cloud from an Theft Attack and detect Abnormal Client Behavior"May2014

[5]. CLOUD SECURITY USING FOG COMPUTING Proceedings of IRF International Conference, 30th March-2014

[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

[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

[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-of- confidential-twitter-documents/ [11] D. Takahashi, "French hacker who leaked Twitter doc- uments to TechCrunch is busted," March 2010. [On- line].

[11]. P. Allen, "Obama's Twitter password revealed after french hacker ar- rested for breaking into U.S.president's account," March 2010.