International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099

VOL 1 ISSUE 1 (2016) PAGES 65 - 70

Received: 12/07/2016. Published: 29/07/2016

Data Security System in Cloud by Using Fog Computing and Data Mining

M. Robert Masilamani[1], P. Valarmathi[2], M. Thamizharasi[3]

[1]Associate Professor, [2,3]Assistant Professor
Department of Computer Science and Engineering
Dhanalakshmi Srinivasan College of Engineering and Technology, Tamil Nadu, India

Abstract

Cloud computing it is outlined as a gaggle of laptop and servers that connected along on network. Today, as several organization and enterprises square measure commencing to adopt the IOT(internet of things),they all want for giant quantity of knowledge to be accessed quickly, to be safe on cloud from assailant or corporate executive then the protection is additionally necessary mechanism to secure cloud knowledge of AN government organization or any IT-industry. Generally existing encoding knowledge protection mechanisms failing in preventing knowledge thievery attacks from criminal assailant, particularly from corporate executive to the cloud supplier. To produce security to cloud knowledge from unauthorized access from malicious assailant we tend to propose a distinct approach to securing knowledge in cloud system by mistreatment decoy technology. We tend to monitor user behavior or knowledge access patterns in cloud system and distinguishing abnormal knowledge access patterns. Once any unauthorized knowledge access patterns is suspected then decoy knowledge is provided to the unauthorized user. This mechanism protects against the misuse of the user real knowledge. If encase real user get at bay during this system then user will raise only once countersign for verification.

Keywords: Fog computing, data processing, clouding up computing, Cloud security.

1. INTRODUCTION

Cloud computing may be a teams of computers and servers square measure connected along over the net. nowadays little or massive organization additionally as several enterprises victimization cloud to store great deal information of knowledge of data it should be non-public data or business information. The necessity of huge quantity of information accessed additional quicker and domestically, is ever growing[2]. This can be wherever the fog computing comes into image. Fog computing may be a term created by Cisco. Fog computing, additionally referred to as fog networking, it's a distributed infrastructure during which bound application services managed at the sting of the network by victimization device and different still managed within the cloud. Primarily it's a middle layer between the clouds and hardware or user finish devices, that providing economical analysis, processing and storage. The goal of fog computing is to enhance potency and scale back the quantity of information that must be transported to the cloud for processing, analysis and storage[1]. If assailants square measure intelligent and launching attack against cloud system then it's straightforward to interrupt cloud user watchword or attacker is malicious corporate executive then it's doable to taken somebody user watchword simply and take a look at to obtaining unauthorized access of cloud system to taken non-public or business data of explicit user. to beat this downside we tend to propose completely different technique to produce security to cloud knowledge from unauthorized user by making confusion by victimization decoy technology[4]. That we've got return to decision fog computing. we will use this technology to launch misinformation attacks against unauthorized user or corporate executive and preventing them to access real user knowledge[3]. In this paper system observation user behavior activity or real user knowledge access patterns if any abnormal knowledge access patterns square measure suspected then fog computing launching misinformation attack against unauthorized user. During this decoy knowledge base square measure full fill with pretend data once any abnormal knowledge access patterns square measure known by system then pretend knowledge from decoy info square measure offer to the invalid user. By victimization this technology we will secure original cloud knowledge from attackers and additionally protects misuse of real user data[5].

2. EXISTING SYSTEM

Following square measure the present system with fog computing.

2.1. Smart grid system:

The fog computing play vital role in smart grid system. During this system as per energy demand, handiness these devices mechanically switch to various energies like star or wind. The Fog collectors at the sting method the information generated by grid devices and sensors and management commands to the actuators. It’s wont to filter the information that is regionally consumed and send to the upper tiers for mental image, transactional analytics and real time report information[6].

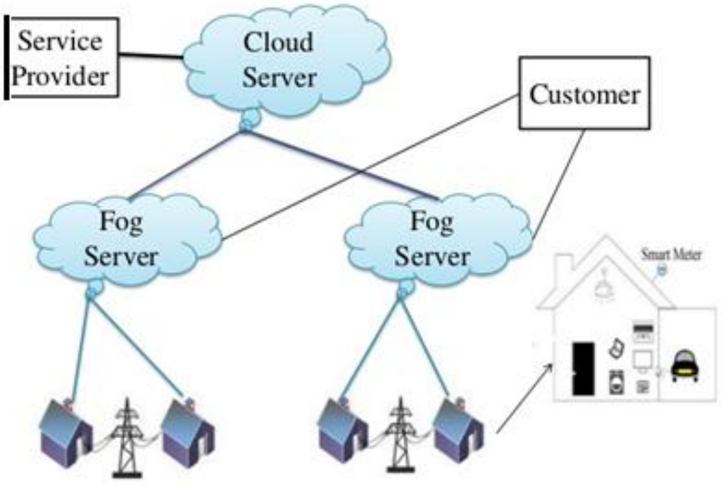

Fig. 1: Example of a Smart Grid System

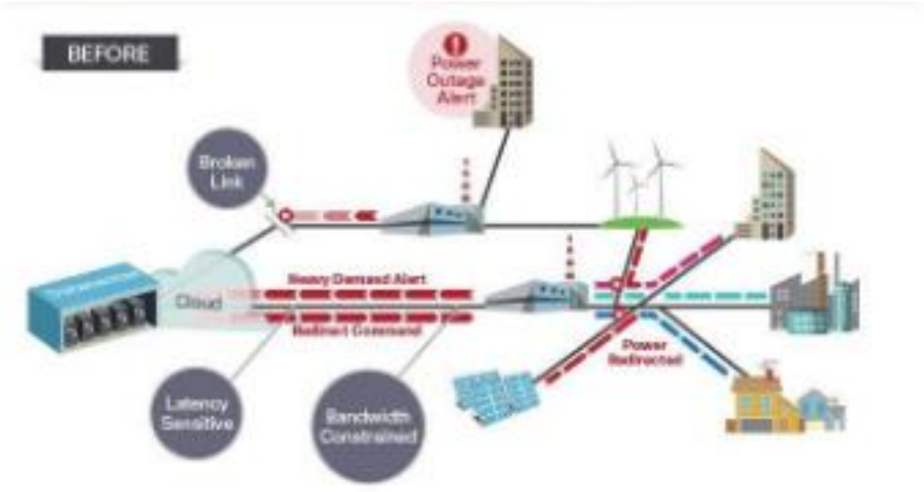

Fig. 2 Existing Fog Computing System

3. PROPOSED SYSTEM

In our proposed system completely different entities illustrated in fig1 information owner consumer, cloud service supplier and cloud server.

1.Data owner: The Data owner is that the real licensed one that hold on personal data or business information on cloud.

2. Cloud server: The cloud server is canopy with fog network ,process the consumer request and grant access on cloud.

3. Admin user : The admin manage user logs, files, produce file signature, manage decoy information base or files.

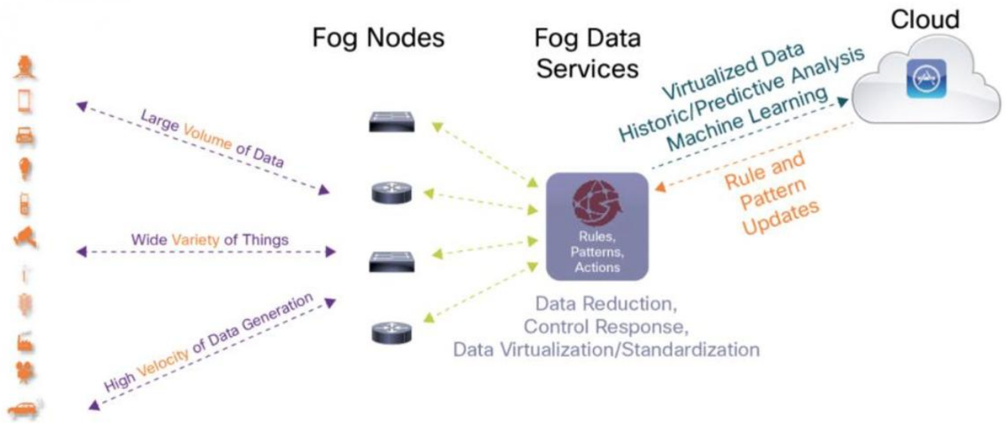

Fig.3. Proposed Model of FOG system

After registration of recent user, consumer obtaining house on cloud and able to perform valid operation on cloud information base like add new files, delete files, transfer files, search files, and invite just one occasion password(OTP) for verification. Whenever user request for information the request received by cloud service supplier before responding consumer request it'll load user profile activity logs and apply mining technique and predict/calculate current request parameters or it'll check user patterns if it's valid then real data square measure given to the user otherwise fog network launching misinformation attack and it'll send faux or fake data to user and this state of affairs forthwith report back to the admin and system logs are updated. however someday there's a clear stage of real user patterns aren't matched that point faux information square measure provides to real user at that point owner of knowledge of information is aware of the system causing decoy data in this state of affairs the important user will raise just one occasion secret (OTP) for verification his identity. The OTP operate conjointly secure with secure hash algorithmic program (SHA-1). This scientific discipline hash operate useful against Man within the Middle Attack (MIM), thus it'll improve the protection of the system. This proposed system conjointly maintains transparency as a result of all the system mechanism is hide from user or wrongdoer. The system admin conjointly perform valid operation like, manage decoy files, produce file signature and update users logs.

4. SECURING CLOUD BY USING FOG NETWORK

Various ways were place for securing information on cloud server by completely different form of techniques. Someday this system has been unsuccessful or unsuccessful in securing user cloud information from corporate executive attackers. And generally different reason additionally inherit image like, miss configuration of services and bugs in code.

4.1. User Behavior Profiling: User identification could be a renowned technique that may be applied here to however a lot of a user accesses their data from cloud information. the system checks ceaselessly traditional user behavior to ascertain whether or not abnormal access or unauthorized access to a user data is going on. Every user encompasses a distinct profile consisting variety of the days user has accessing his files from cloud server. If there's any divergence in user behavior profile that is already holding on in information then it will be known attack is detected[8].

4.2. Decoys: Decoy data it should be pretend documents, trap files, honey files and different pretend data are uploaded by cloud computer user on system. Pretend data contains all false information that produces confusion to assailant. This system is incorporated at the side of user behavior identification. Once unauthorized access is indentified then misinformation attack is launched and decoy information base started providing pretend information to explicit user in such the simplest way that is totally legitimate or legal or traditional. solely true owner user will known once pretend information ar provided by cloud data base then real user will raise just one occasion positive identification for verification[7]. This secures user actual information on cloud and shield from misuse of real information by unauthorized user.

5. BENEFITS AND FUTURE SCOPE

5.1. Advantages:

1. The information hold on on the cloud are often hold on in secured means.

2. The system maintains knowledge integrity.

3. The System shield against misuse of real user knowledge.

4. It'll give security against MIM (Man within the Middle) attacks.

5. This method produce confusion for offender by mistreatment or inserting decoy files in filing system. 6. it'll facilitate to detected smuggled knowledge access

5.2. Future Scope:

1. We will develop robot and IOS application for mobile.

2. To secure cloud knowledge.

3. Study of however attackers behaviors changes in keeping with their information regarding the watching methodology on the target system

4. Knowledge may also be dividing and hold on multiple clouds for further security.

5. Hadoop framework is often used for distributed storage and process of terribly massive knowledge sets.

6. CONCLUSION

An application for securing original cloud knowledge from unauthorized user and providing real or decoy knowledge to user as supported users patterns; here user takes the advantage of the complete feature that square measure provided by this application. For this user merely needed net association to determine reference to cloud knowledge server. this technique distinguishing users real patterns if it's match then this technique offer real knowledge from cloud knowledge server to user and if any unauthorized or offender need to access cloud knowledge then by exploitation fog computing this technique provides decoy knowledge to unauthorized user. encase licensed user obtaining decoy knowledge if user patterns not matching then therein scenario real user will raise just one occasion parole (OTP)for verification. By exploitation this technique personal and business info are often safe from third party user or hackers. All this mechanism operating in background of the system thus this technique maintains transparency, maintain knowledge integrity and make confusion for offender by giving decoy info from decoy knowledge base.

Received: 12/07/2016. Published: 29/07/2016

References

[1] Ben-Salem M., and Stolfo, "Decoy Document Deployment for Effective Masquerade Attack Detection," Computer Science Department, Columbia University, New York.

[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] F. Bonomi, "Connected vehicles, the internet of things, and fog com- puting," in The Eighth ACM International Workshop on Vehicular Inter- Networking (VANET), Las Vegas, USA, 2011.

[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] Ivan Stojmenovic,Sheng Wen "The Fog Computing Paradigm:Scenarios and Security Issues" proceeding of the 2014 federated conference on computer science and information systems pp. 1-8 DOI:10.15439/2014F503 ACSIS,Vol.2.

[6] Manreet kaur, Fog Computing Providing Data Security: A Review, International Journal of Advanced Research in Computer Science and Software Engineering.

[7] Nadhiya Nazeer khan "Fog Computing: A Better Solution For IoT" International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-2, February 2015.

[8] Sayali Raje,Namrata Patil,Shital Mundhe,Ritika Mahajan "Cloud Security Using Fog Computing " Proceedings of IRF International Conference, 30th March-2014, Pune, India, ISBN: 978-93-82702-69-6.