www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 12 Dec. 2016, Page No. 19489-19493

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

Parashar Sangle[1], Romit Deshmukh[2], Rohit Ghodake[3] , Akash Yadav[4] Prof. Jitendra Musale[5]

[1]Abmsp's Anantrao pawar College Of Engineering & Research, Department Of Computer Engineering
parasharsangle@gmail.com
[1]Abmsp's Anantrao pawar College Of Engineering & Research, Department Of Computer Engineering
romitd333@gmail.com
[1]Abmsp's Anantrao pawar College Of Engineering & Research, Department Of Computer Engineering
rohit104064@gmail.com
[1]Abmsp's Anantrao pawar College Of Engineering & Research, Department Of Computer Engineering
akashy2425@gmail.com
[1]Abmsp's Anantrao pawar College Of Engineering & Research, Department Of Computer Engineering
jitendra.musale99@gmail.com

Abstract: Cloud computing it can be defined as a group of computer and servers which connected together on network. Today, as many organization and enterprises are beginning to adopt the IOT(internet of things),they all need for large amount of data to be accessed quickly, to be safe on cloud from attacker or insider then the security is also important mechanism to secure cloud data of an government organization or any IT-industry. Sometimes existing encryption data protection mechanisms failed in preventing data theft attacks from criminal attacker, especially from insider to the cloud provider. To provide security to cloud data from unauthorized access from malicious attacker we propose a different approach to securing data in cloud system by using decoy technology. We monitor user behavior or data access patterns in cloud system and identifying abnormal data access patterns. When any unauthorized data access patterns is suspected then decoy data is provided to the unauthorized user. This mechanism protects against the misuse of the user real data. If incase real user get trapped in this system then user can ask one time password for verification.

Keywords: Fog computing, Data mining, Clouding computing, Cloud security**.**

1. INTRODUCTION

Cloud computing is a groups of computers and servers are connected together over the internet. today small or large organization as well as many enterprises using cloud to store large amount of data it may be private data or business information. the need of large amount of data accessed more faster and locally, is ever growing. this is where the fog computing comes into picture.

Fog computing is a term created by Cisco. Fog computing, also known as fog networking, it is a distributed infrastructure in which certain application services managed at the edge of the network by using device and other still managed in the cloud. Basically it is a middle layer between the clouds and hardware or user end devices, which providing efficient analysis, data processing and storage. The goal of fog computing is to improve efficiency and reduce the amount of data that needs to be transported to the cloud for data processing, analysis and storage.

If attackers are intelligent and launching attack against cloud system then it is easy to break cloud user password or attacker is malicious insider then it is possible to stolen someone user password easily and try to getting unauthorized access of cloud system to stolen private or business information of particular user. to overcome this problem we propose different technique to provide security to cloud data from unauthorized user by creating confusion by using decoy technology. That we have come to call fog computing. We can use this technology to launch disinformation attacks against unauthorized user or insider and preventing them to access real user data. In this paper system monitoring user behavior activity or real user data access patterns if any abnormal data access patterns are suspected then fog computing launching disinformation attack against unauthorized user. In this decoy data base are full fill with fake information when any abnormal data access patterns are identified by system then fake data from decoy database are provide to the invalid user. By using this technology we can secure original cloud data from attackers and also protects misuse of real user information.

.

2. PROPOSED SYSTEM

In our proposed system different entities illustrated in fig1 data owner client, cloud service provider and cloud server.

1.Data owner: The data owner is the real authorized person who stored private data or business information on cloud**.**

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

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

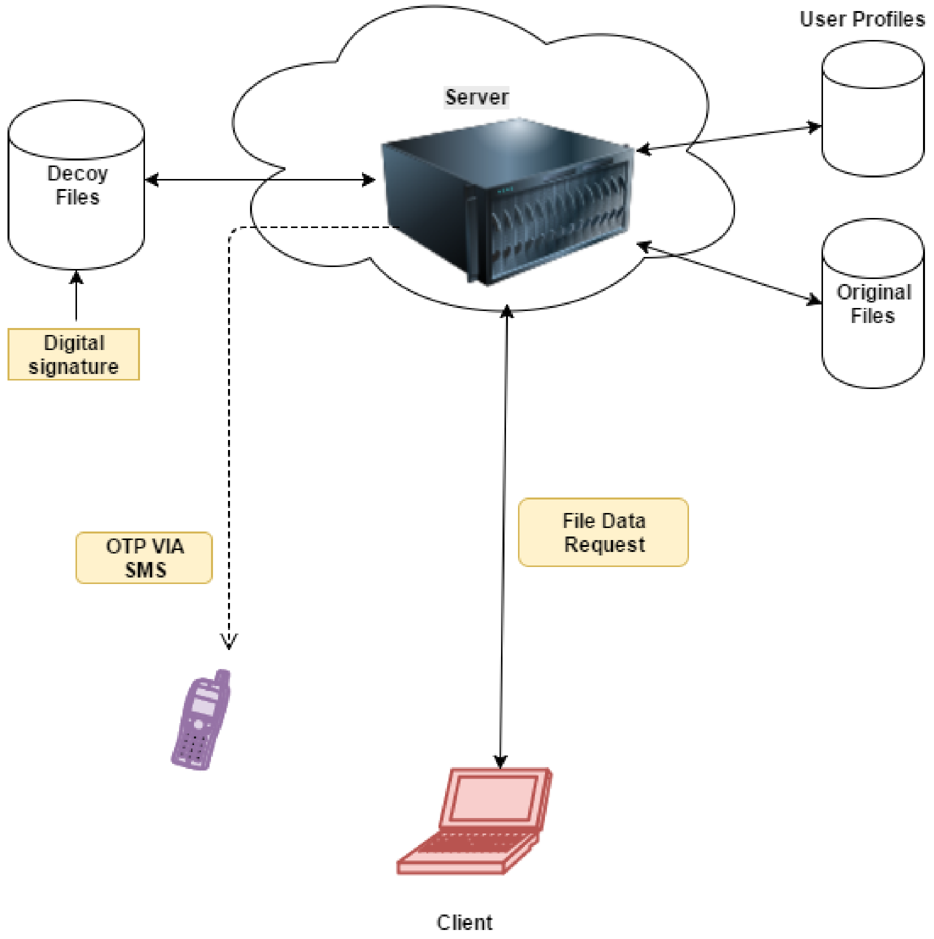

Figure 1: System Model (Proposed system)

After registration of new user, client getting space on cloud and able to perform valid operation on cloud data base such as add new files, delete files, download files, search files, and ask for one time password(OTP) for verification. Whenever user request for data the request received by cloud service provider before responding client request it will load user profile activity logs and apply mining technique and predict/calculate current request parameters or It will check user patterns if it is valid then real information are given to the user otherwise fog network launching disinformation attack and it will send fake or bogus information to user and this scenario immediately report to the admin and system logs will be updated. But sometime there is a possibility of real user patterns are not matched that time fake data are provides to real user at that time owner of data knows the system sending decoy data in that situation the real user can ask one time password (OTP) for verification his identity. The OTP function also secure with secure hash algorithm (SHA-1). This cryptographic hash function helpful against Man In The Middle Attack (MIM), therefore it will improve the security of the system. This proposed system also maintain transparency because all the system mechanism is hide from user or attacker. The system admin also perform valid operation such as, manage decoy files, create file signature and update users logs.

3. EXISTING SYSTEM

Following are the existing system with fog computing.

3.1. Smart grid system:

The fog computing play important role in smart grid system. In this system as per energy demand, availability these devices automatically switch to alternative energies like solar or wind. The Fog collectors at the edge process the data generated by grid devices and sensors and control commands to the actuators. It is used to filter the data which is locally consumed and send to the higher tiers for visualization, transactional analytics and real time report data.

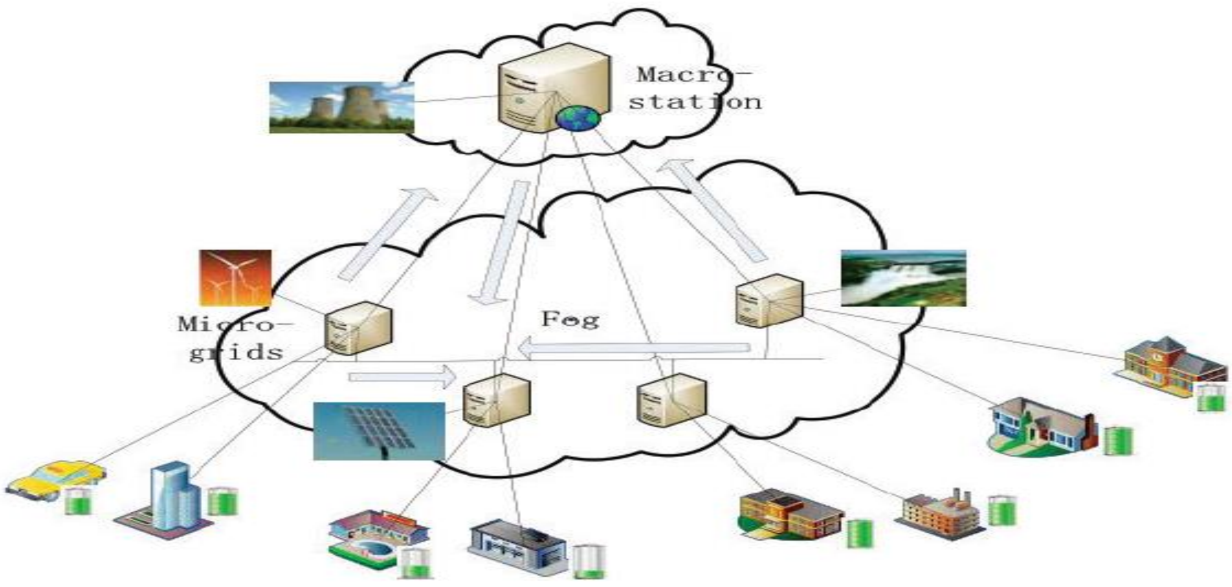

Figure 2: Fog computing in smart grid.

3.2. Smart traffic light system:

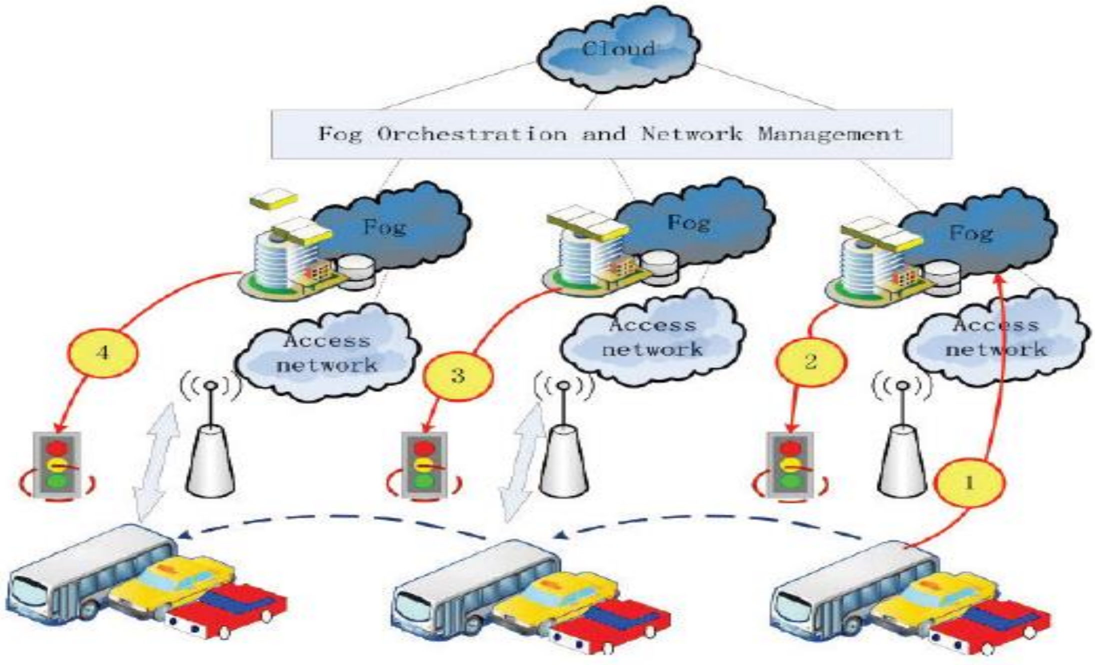

Figure 3: Fog computing in smart traffic light system.

This system has video cameras that sense an ambulance flashing light then it can be automatically change street light and open or clear lanes for the vehicle to pass through traffic. These sensors interact with sensors and it will measure speed and distance of oncoming. This system lighting turns on once sensors identifies movements and turn off as traffic passes. Neighboring smart lights serving as fog devices coordinate to create green traffic wave and it will send warning signals to oncoming vehicles.

4. SECURING CLOUD BY USING FOG NETWORK

Various methods were put for securing data on cloud server by using different type of techniques. Sometime this technique has been failed or unsuccessful in securing user cloud data from insider attackers. And sometimes other reason also come into picture such as, miss configuration of services and bugs in code

4.1. User Behavior Profiling: User profiling is a well known technique that can be applied here to how,when,and how much a user accesses their information from cloud database. the system checks continuously normal user behavior to check whether abnormal access or unauthorized access to a user information is occurring. Each user has a distinct profile consisting number of the times user has accessing his files from cloud server. If there is any divergence in user behavior profile which is already stored in database then it can be identified attack is detected.

4.2. Decoys: Decoy information it may be fake documents,trapfiles,honeyfiles and other fake information are uploaded by cloud system administrator on system. Fake information contains all false data which create confusion to attacker.

This technique is incorporated along with user behavior profiling. When unauthorized access is indentified then disinformation attack is launched and decoy data base started providing fake data to particular user in such a way which is completely legitimate or legal or normal. Only true owner user of data can identified when fake data are provided by cloud data base then real user can ask one time password for verification. This secures user actual data on cloud and protect from misuse of real data by unauthorized user.

5. COMBINING USER BEHAVIOR PROFILING AND DECOY TECHNOLOGY FOR MASQUERADE DETECTION.

5.1. User Behaviors Profiling

The legal user of the system are familiar with the file system and the location where they are stored. Whenever masquerader who gets the access of real user system illegally is unlikely to be familiar with file structure and data or content of that file system. This fake user search is likely to be widespread or untargeted or we can say their search may not to be point.

Basically user search behavior is profiled and developed based on some key assumption. Models are trained with a one class modeling technique i.e one class support vector machine. It will maintain user privacy and securing the user data.

All the real or normal user patterns are is modeled. this model helpful to compare and determine whether the user accessing the system is real user or masquerade.

5.2. Decoy Technology:

All the data within decoy data base are full fill with honey files ,trap files, fake or with bogus information which is uploaded by system admin or cloud service provider of the system.

A masquerader who is unaware with system or file system and location of the data it will try to click on decoy files. Therefore the system is notified of unauthorized activity.

The advantages of placing decoys in a file system.

1. It will helpful to detection of illegal or masquerade activity.
2. It will create confusion to the attacker or insider.
3. The combination of decoy technology and user behavior profiling produce strong proof or evidence of illegal or unauthorized activity of accessing the data and also helpful to improve the accuracy of detection.

The user behavior is identified by using an data access patterns. This pattern may be determined by the number of upload, download count, time of accessing data and session. All this records is maintained by the system. When any users access the system that time his behavior is matched with the user behavior profile which is stored in the database. If the behavior or patterns is matches then we can say that the user is real accessing the data or it said to be user is illegal is accessing the data.

6. ADVANTAGES AND FUTURE SCOPE

6.1. Advantages:

1. The data stored on the cloud can be stored in secured way.
2. The system maintains data integrity.
3. The System protect against misuse of real user data.
4. It will provide security against MIM (Man In The Middle) attacks.
5. This system create confusion for attacker by using or placing decoy files in file system.
6. It will help to detected illegal data access

6.2. Future Scope:

1. We can develop android and ios application for mobile. to secure cloud data.
2. Study of how attackers behaviors changes according to their knowledge about the monitoring method on the target system
3. Data can also be divide and stored on multiple clouds for extra security.
4. Hadoop framework can be used for distributed storage and processing of very large data sets.

7. CONCLUSION

An application for securing original cloud data from unauthorized user and providing real or decoy data to user as based on users patterns; here user takes the advantage of the entire feature which are provided by this application. For this user simply required internet connection to establish connection with cloud data server. This system identifying users real patterns if it is match then this system provide real data from cloud data server to user and if any unauthorized or attacker want to access cloud data then by using fog computing this system provides decoy data to unauthorized user. Incase authorized user getting decoy data if user patterns not matching then in that situation real user can ask one time password (OTP)for verification. By using this system private and business information can be safe from third party user or hackers. All this mechanism working in background of the system therefore this system maintains transparency, maintain data integrity and create confusion for attacker by giving decoy information from decoy data base.

8. 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] 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.

[3] 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.

[4] 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.

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

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

[7] 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.

[8] 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.