International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Oct -2016 www.irjet.net p-ISSN: 2395-0072

Survey On Fog computing :Mitigating Insider Data Theft Attack

Devkar Swapnil, Gokhane Avinash, Kaudare Jaymala , Kambale Shubham, Abhonkar Prashant

[1]*Devkar Swapnil Student, Dept .of Computer engineering, SKNSITS lonavla, maharatra,india*
[2]*Gokhane Avinash Student, Dept .of Computer engineering, SKNSITS lonavla, maharatra,india*
[3]*Kaudare Jaymala Student, Dept .of Computer engineering, SKNSITS lonavla, maharatra,india*
[4]*Kambale Shubham Student, Dept .of Computer engineering, SKNSITS lonavla, maharatra,india*
[5]*Abhonkar Prashant Professor, Dept. of Computer engineering, SKNSITS lonavla, maharatra,india*

Abstract - *Cloud computing is revolutionary something that changes the way we use computer's and smart devices access and storage management despite the cloud there may something still arise of new challenges such like latency lack of mobility support and location awareness etc. Fog computing is promising solution that extends the cloud computing to achieve these different goals. Fog computing is decentralized system that provides cloud computing to edge of network. But existing encryption techniques for data security have failed to secure it from data theft attack especially insider attacker thefts.*

Here we propose the data decoy technology for securing data in the cloud. here we supervise the data access of cloud and detect the unnatural data pattern access pattern. if we caught any kind of unauthorized access then we verify by using challenging questions. even we provide disinformation by large decoy information to attacker to protect user's real data so we are achieve greater level of security.

***Key Words*: Cloud Computing, Decoy, Fog Computing, User Behaviour profiling**

1.INTRODUCTION

In recent time cloud is being used in business sector. so cloud is getting more essential part in human life. But security is big and problem in cloud. In recent that different technology is proposed for security of cloud which fail to provide better security to cloud computing. Especially , insider attack so there might be lot more chance of insider attack. So here we applying the decoy technology with respect to our data for cloud security. In decoy technology misleading the attacker with false information and user behavior profiling for authenticating the user on the basis of different parameters of user behavior with system.

So here we uses two technology for the securing all information on cloud

1.1 PROBLEM STATEMENT

Cloud applied to place data remotely which can be available access of user by some authentication files username and password As we know we can access cloud data from anywhere by internet and even the storage is ,not being used of user space .are all data is online but the thing is that user don't know where and how exact data going to store? what the privacy? The problem will be when the user store sensitive information Quit obviously user will need that kind of assurance of security.

When nobody can right to use view his data and business related information. So encryption technique are applied over cloud but they also not enough more for providing security to users sensitive data.

Twitter incident exposed the security problems in cloud where user of twitter lost their sensitive data and documents within there account password

1.2. EXSTING SYSTEM

Single authentication provided by existing system which is not much more protected that can be easily hacked by attacker. even the present system doesn't verify authentication of user Encryption technique used in present

3. AES ALGORITHM

Advanced encryption standard is uses symmetric block cipher which uses some keys for encryption and decryption This algorithm expects 128 bit block size. The process will be created but in round are identifiable but last round in AES-128 there are 4 different round

involved which are sub-bytes Shift Rows , AddRoundkey In AddRoundKey, Key is added to each byte.

4. RSA ALGORITHM

RSA used for web because from Microsoft and netscap.public log cryptography is used in RSA Public key used encrypy messaged and known to everybody it has 3 main steps

1.key generation

2 encryption

3 decryption

5. PROTECTING CLOUD WITH FOG

different Mechanism are used like encryption ,decryption does not provide reliable security to cloud data. because attacker are strong now days fail these mechanisms. attackers in such technologies easily find key for such encrypted cloud data.

6. USER BEHAVIOUR PROFILING

User behavior profiling is a mechanism that is used to for recognizing when and how frequently the user accesses his data on the Cloud. this mechanism is used continuously detect unauthorized activity. We will let some assumptions of user behavior during access of user which compared with all the parameters result so on that basis we will take decision. if there is deviation in behavior in user profiling which is already stored then attack will detected.

7. DECOY

When are will going to detect attack are misleading the attacker with wrong data by decoy technologies. We will having set of file system with trap in some format of file for which the attacker is seeing and they will believe that they have exfilltrated files and when that decoy file is downloaded by cloud then there will be acknowledge can generate for notify. The decoy files will have honey-pot honey-files , decoy document, various other information related to it.

There are advantage to decoy in file system

1 masquerade activity detection

2 misleading attacker

3 deference effect

8. COMBINING TWO TECHNOLOGY

We will going to provide stronger evidence of malfeasance by combining the search behavior anomaly detection with data decoy technology which is having traps for insider .so therefore we can improve the detection accuracy This combine scenario will cover threat model to illegitimate cloud access

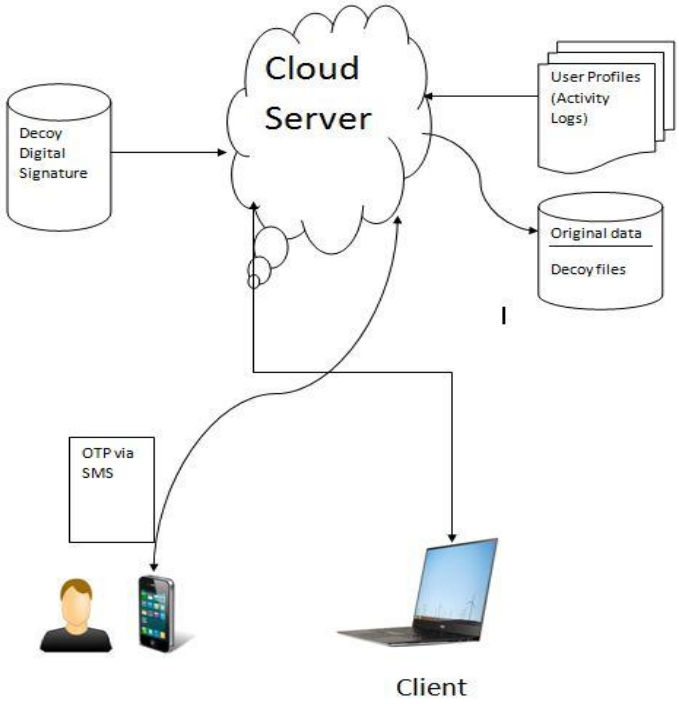

Fig -1: Proposed System

Advantage

1.data stored in server is very reliable

2 this provide privacy

3 insider attack detected

4 attacker doesn't recognize decoy or real information

5 attacker is recognized easily

8. FUTURE SCOPE

We can apply decoy technology for every type of files like picture, audio, video. Data can be divided and stored on different clouds for enabling security .

9. CONCLUSION

In this approach we securing user data in the cloud .we propose data access patterns by profiling user behavior to detect when insider attacker access other user data in cloud service decoy information stored in cloud alongwith the user original data and also used as sensor to detect unauthorized access once unauthorized data access detect and verified by challenge question for instance we provide bogus data to malicious insider to protect users original data

REFERENCES

[1] The Fog Computing Paradigm: Scenarios and Security Issues, Ivan Stojmenovic SIT, Deakin University, Burwood, Australia

[2] FOG COMPUTING:An Approach for avoiding Data Theft by Decoy Information Technology Bhavesh Pandey , Ankit Pawar, Jay Mehta.

[3] Fog Computing: Focusing on Mobile Users at the Edge Tom H. Luan, Longxiang Gao, Zhi Liz, Yang Xiang, Guiyi Wey, and Limin Sunz , School of Information Technology, Deakin University, Australia