FOG Computing: Preventing Insider Data Theft Attacks in Cloud Using User Behavior Profiling and Decoy Information Technology

Gayatri Kalaskar, Purva Ratkanthwar, Prachi Jagadale, Bhagyashri Jagadale.
Department of Computer Enginneering, I2IT college Pune.

***Abstract**: Now a days, Cloud Computing plays very important role in the online world. In Cloud computing gives us significantly different ways of using computers to access our personal and business information. These new ways also arises some new challenges in security of cloud. Old techniques like data encryption have failed in preventing data theft where the perpetrator are insider to the cloud provider.*

We are proposing a new approach where data is secured by offensive decoy technology. We monitor different parameters of data access in cloud to detect data access patterns. When unauthorized data access is suspected and then verified by using challenge questions, we send large amount of decoy information to attacker. This decoy information prevents misuse of user's real data.

Keywords: ***Fog Computing, Decoy Security, Decoy Information Technology.***

1. Introduction

Now a days, Cloud is very essential need of all organization and firms. Cloud can store very large amount of data of organizations and firms so they can access data from anywhere in world by only internet connection with them. Cloud has benefits as well as some challenges of securing data in cloud. Problems of hacking cloud can lead to misuse of personal data and organization's important data. Mostly hacker is insider to the organization or person with negative thoughts and bad intention.

The twitter incident is example where the personal and important data is hacked and launched on the incorporate website. In this incident, accounts of users were hacked including the account of U.S. President Barack Obama.

So to prevent this data theft attacks in cloud, we are introducing new technique called fog computing. In this technique, we are introducing the combination of two technologies: User Behavior Profiling and Decoy Information Technology.Using User Behavior profiling technology, we detects authorized and unauthorized person. If the person is authorized then it sends the original file but if the person is unauthorized then it sends the bogus files.Unauthorized person doesn't know that files are bogus files. To secure the real data of the user frommisuse we can use decoy file technology.

2. Literature Survey

The existing system is less secure and can be easily hacked by anyone professional in hacking field. Facility of security questions has been provided to the existing system then also the existing system is very less secure. Anyone who has got unauthorized access to cloud can search for files and data. The system is not able to identify whether the user is legitimate or not. If the person is illegitimate then also this system sends the original information. Therefore existing system is not secure. Encryption is provided to existing system but cloud and data is not secure by only encryption.

Paper Title	Abstract	Advantages
Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud	Monitor data and provides data security from intruders and helps in confusing the attacker about the real data.	1-User Behavior Profiling 2-Decoy Information technology
Software decoys for insider threat	Discussed a technique that confuses the insider and also used obfuscation which helps to secure data by hiding it and making it decoy information for insider	Developed a technique that was a software decoy for securing cloud data
Reliability in the	Provides	Three tier architecture

Utility Computing Era: Towards Reliable Fog Computing	feasibility to real time objects.	for Fog Computing is used.
Improving Websites Performance using Edge Servers in Fog Computing Architecture	Various methods are combined and used with unique knowledge to improve the performance of rendering a web page	Reducing the size of web objects, minimizing HTTP requests, and reorganizing the web page.

2.1Problems in Cloud:

1. Data loss: Data loss occurs when disk drive dies without any backup created by cloud owner. It usually occurs when the encrypted key is not available with owner.
2. Account traffic hijacking: It usually occurs when the login credentials are lost and then account can be hijacked.
3. Denial of service: This usually occurs when large amount of users requesting for same service and hacker takes advantage of this situation for hijacking.
4. Malicious insider: This lead to misuse of login credentials by known person in contact.
5. Shared technology: This occurs when many websites shares same information or data.
6. Misuse of cloud services: By using many cloud servers, hackers can be able to crack the encryption in very small amount of time.
7. Insufficient knowledge: Many firms and organization jump into the cloud without knowing the advantages and disadvantages of the cloud which lead them to data loss.

3. Proposed System

Proposed system uses user behavior profiling and decoy information Technology. It firstly deals with the user's behavior, system checks that the user is legitimate or not. If system find unauthorized person then it sends decoy data and keep user's real data safe.

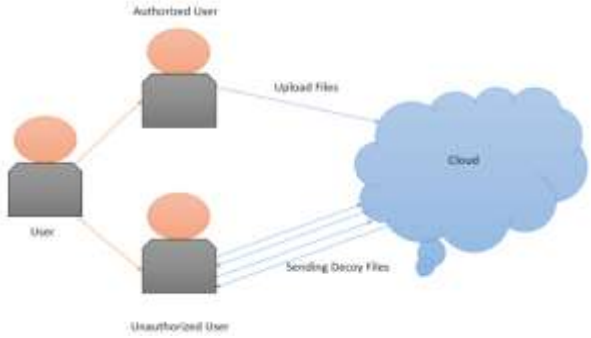


Fig. 1 ***Proposed System***

3.1 User Behavior Profiling:

User behavior profiling deals with the behavior of the user.They monitor data access in the cloud and detect abnormal data access pattern.

User profiling will a well known technique that can be applied here to check how, when and how much a client access their data in the cloud. Such normal user behavior can be continuously checked to determine whether abnormal access to a user's data is experience.

In other words, When any person get access in the cloud, then our system start detecting behavior of that person on the basis of following characteristics:

1. Login Time
2. Session Time
3. Upload Count
4. Download Count
5. How many files he will read and how often.

System compares all above new data set with predefined data sets which we store in the database and identify that person is authorized person or not and according to that system will send the data.

3.2 Decoy Information Technology:

We are using decoy information technology for sending the decoy information to the unauthorized user. Using user behavior profiling, when system find person's behavior is not matches with the predefined data set then system get to know that person is unauthorized.so here, we can apply decoy information technology to secure the real data.

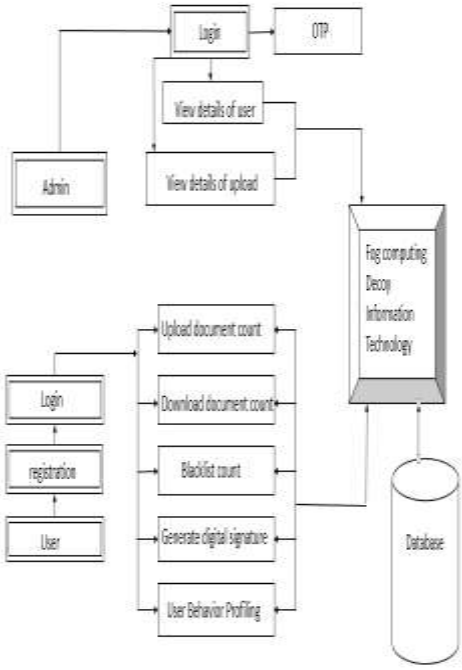
When unauthorized person found,system sends the bogus data to that person.person assumes that bogus data as original data.

Blacklist Count:

System also detects how many unauthorized person accessing the account of authorized person and add the count according to that in the blacklist count.

Only authorized person have access to clear that blacklist count. When unauthorized person want to clear that count then system will send OTP to the authorized person**.**

Advantage of placing decoy files in database are:



1.The detection of unauthorized person's activity.
2.The confusing the attacker with bogus data.
3.Send bogus files.

4. Mathematical Model

Let,

G be the superset of all sets.

G ≡ {input, output, operations, success, failure}

Where ,

Input is set of parameters provided as input to system.

Input ≡ {U, S, DS, F}

U is set of users. It is infinite set of users.

U ≡ {U1, U2, U3……Un}

S is set of servers. It is finite set of servers.

S ≡ {S1}

DS is set of dataset parameters.

DS ≡ {P1, P2, P3, P4, P5}

P1 ≡ Session Time

P2 ≡ Duration

P3 ≡ File upload count

P4 ≡ File Download count

P5≡ Blacklist count

F is set of files. It is Infinite set of files.

F ≡{F1, F2, F3……., Fn }

Output is set of results.

Output ≡ { Legal user/Unreal user, Decoy document, Alert user via mail, OTP via SMS }

Operations is set of functions.

Operations ≡ { Op1, Op2, Op3, Op4, Op5, Op6, Op7, Op8, Op9}

Op1 ≡ Request received

Op2 ≡ Load user profile

Op3 ≡ Apply mining & calculate current request parameter

Op4 ≡ if invalid user then send the Decoy/Bogus data

Op5 ≡ Fetch file

Op6 ≡ Calculate digital signature

Op7 ≡ Compare with decoy file digitally

Op8 ≡ If similar, Alert admin

Op9 ≡ Update log, Blacklist

SUCCESS ≡ Desired input generated

FAILURE ≡ Desired output not generated

4. Conclusion

In this paper, we propose a unique approach for securing users data in cloud. We are securing organizations and firm's important data in cloud by using combination of two technologies. We are mapping user behavior by different patterns and we distinguish real user and fake user. So we can provide more security the data in cloud. If fog system finds unauthorized access to the account then decoy information will be send to the unauthorized user. This technology will add level up security in cloud system.

References

1) Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data theft Attacks in Cloud" IEEE 2012
2) Ivan Stojmenovic, Sheng Wen, "The Fog Computing Paradigm: Scenarios andSecurity Issues" IEEE 2014
3) 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 Available online@www.ijcta.com
4) Thogaricheti Ashwini, Mrs. Anuradha.S.G, "Fog Computing to protect real and sensitivity information in Cloud", IJECSE | SSN 2277-1956/V4N1-19-29
5) Shanhe Yi, Cheng Li, Qun Li, "A Survey of Fog Computing: Concepts, Applications andIssues, ACM 2015
6) Viraj G. Mandlekar, VireshKumar Mahale, Sanket S.Sancheti, Maaz S. Rais, "Survey on Fog Computing Mitigating Data TheftAttacks in C loud", International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-2, Issue-6, November-2014
7) Yongkun Li, Member, IEEE, and John C. S. Lui, Fellow, IEEE, "Friends or Foes: Distributed and RandomizedAlgorithms to Determine DishonestRecommenders in OnlineSocial Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 10, OCTOBER 2014
8) Manreet kaur, Monika Bharti, "Fog Computing Providing Data Security: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014
9) Divya Shrungar J, Priya M P, Asha S M, "Fog Computing: Security in Cloud Environment", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, August 2015
10) Younghee Park, Salvatore J. Stolfo, "Software Decoys for Insider Threat", ACM 2012
11) Miss. Shafiyana Sayyad, Mr.Anil Bhandare, Mr. Deepak Yelwande, "Fog Computing:Software decoys for insider threat", Volume 2 issue 3 March 2015
12) Tom H. Longxiang Gao, Yang Xiang, Zhi Li, Limin Sun, "Fog Computing: Focusing on Mobile Users at the Edge" 6 Feb 2015
13) Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli, "Fog Computing nd Its Role in the Internet of Things", ACM 2012
14) Manreet Kaur, monika Bharati, "Securing user data on cloud using Fog Computing and Decoy technique", Volume 2, Issue 10, October 2014