Survey on Fog Computing Mitigating Data Theft Attacks in Cloud

Viraj G. Mandlekar, VireshKumar Mahale, Sanket S.Sancheti, Maaz S. Rais

Abstract: **Cloud computing now-a-days forms a very important unit in the online world, by modifying how the computers and Internet were used few years back. Cloud computing provides the facility to store personal information and the information related to the business firms along with its access from anywhere in the world. In event of providing the facility cloud has many drawbacks related to its security which is mainly termed as data theft attacks. Especially these drawbacks are more offensive when done by an insider.**

So to overcome these drawbacks we are proposing a new technology called Fog Computing. Fog Computing forms a single unit by dealing with two different technologies i.e. User Behavior Profiling and Decoy Information Technology. Using these technologies we detect the behavior of the user and compare it with the normal user behavior. Along with this we provide authentication by various challenge questions so that hacking the login credentials does not log into the account. Besides this if any unauthorized access is detected providing with the fake data so that real data should be saved from hacking. Thus provides higher levels of security to the cloud.

Keywords- **Cloud, encryption, decoys behavior profiling, blowfish, aes, rsa.**

1. INTRODUCTION

Cloud now-a-days forms a basic need of all the firms or organizations that deal with storing of large amount of data, so most of the firms are opting for cloud. Cloud forms to be very efficient in storing large amount of data and providing access to it from anywhere in the world just with an availability of an internet connection. Cloud being famous has some problems of hacking which leads to an unauthorized access to the personal data or the firms important data. Cloud can even be hacked by an insider i.e. a person close to us with negative thoughts [8].

In short the cloud is a beneficial technology but has the problems of data theft. The Twitter incident is an example of data theft in which the personal and important data was launched on an incorporate website [5], [9], and the accounts of customers were accessed illegally including the account of U.S. President Barack Obama [6], [7].

So to overcome these problems we are introducing a new technology called Fog Computing. Fog Computing deals with two technologies to avoid unauthorized access they are, User Behavior Profiling & Decoy Information Technology. These technologies will help us in detecting the abnormal behavior of the hacker and providing with fake information to keep the data safe from misuse. These technologies will authenticate the user not just by the login credentials but also with the security questions that are previously set by the user. If the credentials and the security questions are not dealt properly the data provided will be in the encrypted format and it will be unreadable to the unauthorized user.

2. LITERATURE SURVEY

2.1. Existing System: The present system provides only the single authentication which is not much secure and can easily be hacked by a hacker. The system does not provide any additional security like security questions for more security. The hacker can easily get into the cloud and search for the files that are available. The present system does not verify whether the user is authorized or not. The existing system provides security by encryption but it fails to secure the cloud.

Threats in cloud:

1. Data breaches – This led to the loss of personal data and credit card information of about 110 million people, it was one of the theft during processing and storage of data.
2. Data loss – Data loss occurs when the disk drive dies without any backup created by the cloud owner. It occurs when the encrypted key is unavailable with the owner.
3. Account or service traffic hijacking – Account can be hacked if the login credentials are lost.
4. Insecure API’s – Application Programming Interface controls the third party and verifies the user.
5. Denial of service – This occurs when millions of user request of same service and the hackers take this advantage for hacking.

6. Malicious insiders – This occurs when a person close to us knows our login credentials.
7. Abuse of cloud services – By using many cloud servers hacker can crack the encryption in very less time.
8. Insufficient due diligence- Without knowing the advantages and disadvantages of the cloud many businesses and firms jump into cloud thus leading to data loss.
9. Shared technology – This occurs when the information is shared by the many sites [8].

2.2. Commonly used encryption techniques in present:

2.2.1. Blowfish Algorithm

Blowfish is a symmetric block cipher encryption algorithm. In this algorithm same secret key is used for encryption and decryption. The messages are divided into fixed length blocks for encryption and decryption. Block length used in blowfish is 64 bits. The key can be of length up to 448 bits. Messages that are not in the multiples of 8 bytes are to be padded. This algorithm suits better for the applications where the key does not change constantly. It best suits for communication link or automatic file encryptor. This algorithm works faster as compared to other algorithms when is it put on to 32 bit microprocessors with large data caches [12].

Disadvantage:

Once the source code is obtained easy to hack the encryption.

2.2.2. AES Algorithm

Advanced Encryption Standard is a symmetric block cipher. This algorithm uses same keys to encrypt and decrypt. The algorithm expects a block size of 128 bits.

The algorithm provides with the choice of three keys – 128, 192, 256 bits. The standard which is used decides the name AES-128, AES-182, AES-256.Processing for encryption is carried out in 10 rounds for AES-128, 12 rounds for AES-192, and14 rounds for AES-256 bit keys. All the rounds are identical except the last rounds in each case. There are Four rounds involved called SubBytes, ShiftRows, MixColumns and AddRoundKey.

In SubByte round entry is kept of which byte is replaced with which into an lookup table. In ShiftRow the rows are shifted cyclically but the first row is kept unchanged. The bytes in the second third and fourth rows are shifted by an offset of one two and three respectively. In MixColumns round each column containing four bytes are mixed using an invertible linear transformation and the output is generated. In AddRound Key, key is added to each byte. Last three steps are repeated again except the last round [14].

Disadvantage:

1. Algorithm requires more processing.
2. It requires more rounds as compared to other algorithms.

2.2.3. RSA Algorithm

RSA algorithm is most commonly used to encrypt and to authenticate. It has been also used as Web browser from Microsoft and Netscape. RSA uses public key cryptography; it involves private key and public key. The public key is used to encrypt the messaged and can be known to everybody. RSA algorithm involves three main steps Key Generation, Encryption, Decryption.

In this algorithm two large prime numbers are multiplied with additional operations results into a set of two numbers which contains a public key and other set contains a private key. Public and private keys are required to encrypt and decrypt with only the owner should know it. In this algorithm private key is not sent over the internet. The main role of private key is to decrypt the text that has been previously encrypted by a public key.

Disadvantage:

1. Complexity of key generation.
2. Security needs to be proved.
3. Slow of the speed.

3. METHODOLOGY

3.1. Proposed System: The proposed system has the objective to validate the access is authorized or not and if abnormal access is detected than providing the hacker with encrypted or unreadable information. Fog Computing deals with two technologies User Behavior Profiling and Decoy Information Technology.

3.1.1. User Behavior Profiling

As the name implies the technology deals with detecting the unauthorized access by checking the behavior of the user. The authorized user will only access the files which are related to his work and the other files will be of no use for him. The normal user will only work on the files of his need and will have no work with other files.

If the abnormal user hacks the cloud than the hacker will have no idea about the files and how often they are used and which all accounts mostly access these files. The hacker will try to access the files that are related to different accounts. Even more the access of the hacker will be in the abnormal pattern. This simple scenario is used to detect the abnormal behavior of the user thus providing better security for saving the important data [4].

3.1.2. Decoy Information Technology

Key Hashed Message Authentication Code Algorithm (HMAC):

Decoy Information technology works on the algorithm Key Hashed Message Authentication Code (HMAC). If the hacker gets the success to hack the username and password he tries to access the files but before that he has to cross one more barrier of security question which has been randomly set by the user. Even if the hacker tries and enters anything he gets the access to the account but the data displayed will be in the encrypted format. Here the terminology is that a key will be generated every time during entering the security question. This key will be matched every time the key generated during previous login will be matched with the key generated during next login. If the security question entered is correct then same key will be generated and will have access to the data but if the security question falls to be wrong then the key will not be same and thus will have data displayed in encrypted format and the original data will be kept safe on cloud. This will prevent the unauthorized user to hack the data [11].

4. MATHEMATICAL MODEL

- Let us consider that we have database ‘D’ and ‘n’ number of attribute such as user name, user id etc.

$$\mathbf{D = \{A | A\ \varepsilon\ \text{Information of user}\}}$$

Here D is the set of all A such that A is information of user which is to be store on server

Consider following function

STORE (D, SERVER): Here admin enter the user information into database at server.

Let us consider that the receiver provide us with value “X” for every input it obtain from the every time login account of the particular user .so we can further assume to have a set ‘s to have value ’n’ number of detect value at particular instance.

Let us denote the current situation in the following manner

$$\mathbf{S = \{X | \forall\ X\ \varepsilon\ D\ \exists\ ID\ \text{for attacker}\}}$$

Here S is the set all X such that for all X there exits Id for user.

Now, for some X value that match with some value inside the database when admin check user account update.

1. GET(D,X,SERVER): Admin get all information about the user account from server.

2. PUT(X,ATK,SERVER): Here admin will upload attacker’s information on server.

3. PUTP(X,REPORT,SERVER) : Here admin upload daily report on server.

5. CONCLUSION

Thus in this paper we propose a distinct technology to make the cloud safer by securing the personal and the important data of the business firms. We provide monitoring of the access to the account by checking the behavior of the user. We provide access not only by login credentials but also by challenge questions which would be only known to the user. If the access found to be unauthorized thus providing with the fake data so that the real data of the user can be saved. This technology would add up a level in securing the data on the cloud.

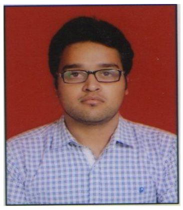
REFERENCES

1. Salvatore J. Stolfo, Malek Ben Salem, Angelos D. Keromytis, “Fog Computing Mitigating Inside Data Theft Attacks In The cloud”,IEEE Base Paper, 2013
2. F. Rocha and M. Correia, “Lucy in the sky without diamonds: Stealing confidential data in the cloud,” in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments, Hong Kong, ser. DCDV ’11, June 2011.
3. M. Van Dijk and A. Juels, “On the impossibility of cryptography alone for privacy-preserving cloud computing,” in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec’10. Berkeley, CA, USA: USENIX Association,pp. 1–8, 2010.
4. M. Ben-Salem and S. J. Stolfo, “Modeling user search-behavior for masquerade detection,” in Proceedings of the 14th International Symposiumon Recent Advances in Intrusion Detection. Heidelberg: Springer,pp. 1–20,September 2011.
5. D. Takahashi, “French hacker who leaked Twitter documents to TechCrunch is busted,” March 2010.
6. D. Danchev, “ZDNET: french hacker gains access to twitter’s admin panel,” April 2009.

7. P. Allen, “Obama’s Twitter password revealed after french hacker arrested for breaking into U.S. president’s account,” March 2010.
8. Cloud Security Alliance, “Top Threat to Cloud Computing V1.0,” March 2010.
9. M. Arrington, “In our inbox: Hundreds of confidential twitter documents,” July 2009.
10. J. Pepitone, “Dropbox’s password nightmare highlights cloud risks,” June 2011
11. B. M. Bowen and S. Hershkop, “Decoy Document Distributor”.
12. Ali Ahmad Milad, Hjh Zaiton Muda, Zul Azri Bin Muhamad Noh, Mustafa Almahdi Algaet,” Comparative Study of Performance in Cryptography Algorithms” Journal of Computer Science 8 (7): 1191-1197, 2012 ISSN 1549-3636, Malaysia, 2012
13. M. Ben-Salem and S. J. Stolfo, “Combining a baiting and a user search profiling techniques for masquerade detection,” in Columbia University Computer Science Department, Technical Report # cucs-018-11, 2011.
14. M.Pitchaiah, Philemon Daniel, Praveen, “Implementation of Advanced Encryption Standard Algorithm”, International Journal of Scientific & Engineering Research Volume 3, Issue 3, ISSN 2229-5518, March 2012.
15. Etikala Aruna, Dr. Ch GVN Prasad, A. Malla Reddy,“ International Journal of Advanced Research in Computer Science and Software Engineering”, Volume 3, Issue 9, ISSN: 2277 128X, Hyderabad (INDIA), September 2013

Viraj Girish Mandlekar
(Student),Final year (BE Computer)
Sandip Institute of Technology &
Research Center, Nashik

Vireshkumar Mahale
(Student),Final year (BE Computer)
Sandip Institute of Technology &
Research Center, Nashik



Sanket Satish Sancheti
(Student),Final year (BE Computer)
Sandip Institute of Technology &
Research Center, Nashik

Maaz Shad Rais
(Student),Final year (BE Computer)
Sandip Institute of Technology &
Research Center, Nashik