Detection And Intimation of Theft (Banking)

Dr. Nilesh T. Gole[1], Chanakshi N. Mendhekar[2], Prajwali A. Shinde[3], Apesksha H. Begde[4], Shital D. Gayakwad[5], Dipali V. Dharmik[6]

[2,3,4,5]Department of Computer Science & Eng. Vidarbha Institute of Technology, Umred Road, Nagpur, India

[1]Associate professor, Department of Computer Science & Eng. Vidarbha Institute of Technology, Umred Road, Nagpur, India

Abstract-Cloud computing promises to significantly change the way we use computers and access and store our personal and business information. With these new computing and communications paradigms arise new Cyber Security challenges. Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the cloud provider. We propose a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. Experiments conducted in a local file setting provide evidence that this approach may provide unprecedented levels of user Cyber Security in a Cloud environment.

Keywords:- ***cloud computing, fog computing, decoy technique, insider theft attacks.***

I.INTRODUCTION

Businesses, especially startups, and small-medium businesses (SMBs), are increasingly opting for outsourcing data and computation to the Cloud. This obviously supports better operational efficiency but comes with greater risks, perhaps the most serious of which is data theft attacks.

Data theft attacks are amplified if the attacker is a malicious insider. This is considered as one of the top threats to cloud computing by the Cloud Security Alliance. While most Cloud computing customers are well aware of this threat, they are left only with trusting the service provider when it comes to protecting their data. The lack of transparency into, let alone control over, the Cloud provider's authentication, authorization, and audit controls only exacerbate this threat. The Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were ex-filtrated to the technological website Tech Crunch and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed. The attacker used a Twitter administrator's password to gain access to Twitter's corporate documents, a security problem that, to date, has not provided the levels of assurance most people desire. Many proposals have been made to secure remote data in the Cloud using encryption and standard access controls. It is fair to say all of the standard approaches have been demonstrated

to fail from time to time for a variety of reasons, including insider attacks, misconfigured services, faulty implementations, buggy code, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures. Building a trustworthy cloud computing environment is not enough, because accidents continue to happen, and when they do, and information gets lost, there is no way to get it back. One needs to prepare for such accidents

OBJECTIVE AND SCOPE OF REVIEW

We propose a completely different approach to securing the cloud using decoy information technology, which we have come to call Fog computing. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing real sensitive customer data from fake worthless data. The decoys, then, serve two purposes: (1) validating whether data access is authorized when abnormal information access is detected. (2) confusing the attacker with bogus information.

II. LITERATURE REVIEW

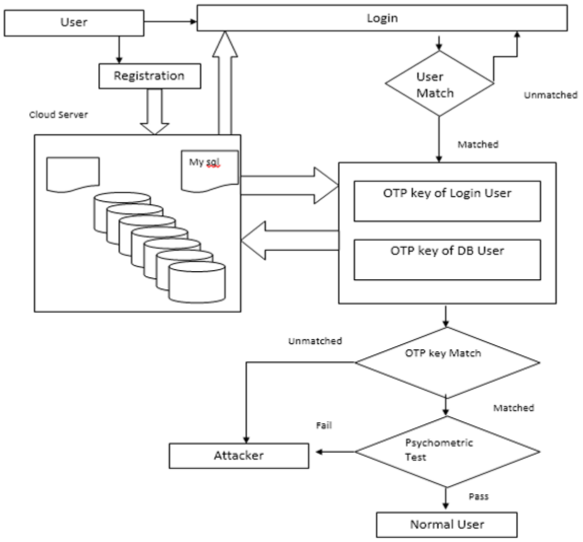
The present system provides only a single authentication which is not much secure and can easily be hacked by a hacker. The system does not provide any additional security like security questions for more security. The hacker can easily get into the cloud and search for the available files. The present 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 clouds: 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 thefts during the 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 to the owner. 3. Account or service traffic hijacking – the Account can be hacked if the login credentials are lost. 4. Insecure APIs – Applications Programming Interface controls the third party and verifies the user. 5. Denial of service – This occurs when millions of users request the same service and the hackers take this advantage to 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 hackers 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 the cloud thus leading to data loss. 9. Shared technology – This occurs when the information is shared by the many sites

III. PROPOSED METHODOLOGY

The proposed system has the objective to validate whether the access is authorized or not and if abnormal access is detected then providing the hacker with encrypted or unreadable information. Fog Computing deals with two technologies User Behaviour Profiling and Decoy Information Technology.

- USER BEHAVIOUR PROFILE AS :
  The name implies the technology deals with detecting unauthorized access by checking the behaviour 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 then the hacker will have no idea about the files and how often they are used and which alls 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 an abnormal pattern. This simple scenario is used to detect the abnormal behaviour of the user thus providing better security for saving the important data [4].
- 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 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 the previous login will be matched with the key generated during the next login. If the security question entered is correct then the same key will be generated and will have access to the data but if the security question fails to be wrong then the key will not be the same and thus will have data displayed in an encrypted format and the original data will be kept safe on cloud. This will prevent the unauthorized user to hack the data.

- SYSTEM FLOW DIAGRAM:



IV. COMBINING TWO TECHNIQUES

The correlation of search behaviour anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy. We hypothesize that detecting abnormal search operations performed before an unknown suspecting user opens a decoy file will corroborate the suspicion that the user is indeed impersonating another victim user. This scenario covers the threat model of illegitimate access to Cloud data. Furthermore, an accidental opening of a decoy file by a legitimate user might be recognized as an accident if the search behaviour is not deemed abnormal. In other words, detecting abnormal search and decoy traps together may make a very effective masquerade detection system. Combining the two techniques improves detection accuracy.

MODULES:

There are four types of modules based on this application as follows:

CLOUD COMPUTING

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction. It is divided into three types,

1. Application as a service.
2. Infrastructure as a service.
3. Platform as a service.

V. CONCLUSION

we present a novel approach to securing personal and business data in the Cloud. We propose monitoring data access patterns by profiling user behaviour to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service. Decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information to dilute the user's real data. Such preventive attacks that rely on disinformation technology, could provide unprecedented levels of security in the Cloud and social networks.

REFERENCE

[1] Hashizume K., Rosado D. G., Fernandez- Medina E. and Fernandez E. B. “An analysis of security issues for cloud computing”. Journal of Internet Services and Applications, 2013, 4(1), pp. 1-13.

[2] Marinos A. & Briscoe G., Community Cloud Computing (pp. 472-484). Heidelberg: Springer, 2009, pp. 472-484.

[3] Archer, Jerry, et al. "Top threats to cloud computing v1. 0." Cloud Security Alliance (2010).

[4] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.

[5] Madsen, Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013.