Secure File Hosting in Private Cloud Services

Nangunuri Raghu[1], Daithala Sreedhar[2], Prashanth Kumar D[3]

Asst.Prof in CSE Department, Kamala Institute of Technology & Science, Singapur, Huzurabad, Karimnagar[1,3]

Asso.Prof in CSE Department, Vidya Bharathi Institute of Technology, Pembarthi, Jangaon, Warangal[2]

ABSTRACT

Cloud computing provides services in wide range for business firms. Nowadays small and medium businesses firms are depending for their data services and computation on out sourcing of on cloud. The cloud provides a very high efficient services for the business organizations. These business organizations trust cloud service providers for their data security. Providing security is highly risk in cloud, especially in private cloud services. Existing data security methods are not so effective. They are failed in preventing theft attacks.

This paper propose a new approach for securing file hosting in private cloud service. OTFP – "One Time File Password" is an Email service that protects unauthorized access of file hosting account and file downloading form the cloud.

General Terms

Cloud computing, security, private cloud

Keywords

Cloud computing, security, private cloud, second party security, OTFP.

1. INTRODUCTION

Newly starting business organizations are mainly depending for their data services on cloud on outsourcing. These business organizations are selecting the best cloud service providers. This makes operational efficiency and less risk for business organizations. Even though there is less risk for business organizations, there is chance of data theft risk which will be responsibility of cloud provider. Data theft attackers may attack the cloud for stealing important business data.

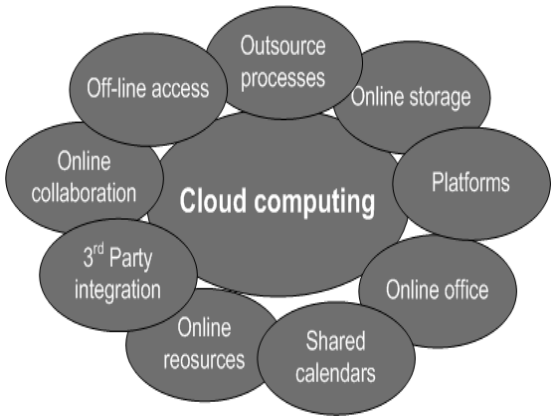

Figure 1: Cloud Services

Figure1 shows about cloud services. The threat of a malicious insider [1] who tries to attack is well-known to most business organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it can monitor these employees, or how it can analyze and makes report on policy compliance. To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or to gain complete control over the cloud services with little or no risk of detection.

Some free file hosting websites like mediafire.com, ziddu.com, 4shared.com etc are providing free file hosting service on cloud. if hacker knows the user login name and password he may attack and he may steal all the files.

1.1 Twitter Incident

The Twitter incident is one example of a data theft attack in the cloud services. Several Twitter corporate and personal documents were ex-filtrated to technological website TechCrunch [2], [3], and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed [4], [5]. The attacker used a Twitter administrator's password to gain access to Twitter's corporate documents, hosted on Google's infrastructure as Google Docs. The damage was significant both for Twitter and for its customers.

1.2 How the Attacker Attacks

The attacker who tries to steals password of user login. To get this password generally the attackers uses trial and error method. The attacker tries the user's names, pet names, date of birth, car number, phone number etc. by combining these details the attacker tries password.

Rocha and Correia explained that how it is easy to steal passwords by a malicious insider of the Cloud service [6]. They also demonstrated how Cloud customers' private keys can be stolen, and how their confidential data can be extracted from a hard disk or data storage device. After stealing a customer's password and private key, the malicious insider will get full access to all the customer data, while the customer is unable of identifying and detecting this

unauthorized access. The malicious insider will tries to logins in odd time i.e. when actual user in off status the attacker will gets login to users cloud service account. This makes the actual customer loss of his data which may lead to damage or loss of his business organization.

Much research in Cloud computing security has focused on ways of preventing unauthorized and illegal access to data by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data theft attacks. Van Dijk and Juels have shown that fully homomorphic encryption, often acclaimed as the solution to such threats, is not a sufficient data protection mechanism when used alone [7]. The homomorphic encryption, private key method and other techniques has failed in cloud service security.

1.3 Fog Computing

Prof .Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis have proposed "Fog Computing [8]" for avoiding malicious insider attacks. They proposed by using of user profiling and decoy technology, so that it can avoid malicious insider theft attacks. But in some of times authorized user may lose his valuable time and he may need to answer some number of questions posed by system.

1.4 Proposal

This paper proposes a new unique approach in cloud computing "OTFP – One Time File Password". This OTFP prevents attacks such as the Twitter attack, by not allowing unauthorized user to access or download the private documents (like social networking profile) within the Private Cloud.

2. SECURING CLOUD

The main service of cloud is to store documents; media files etc. cloud provides public cloud and private cloud. When the files are stored in public cloud such files will not have security as they can be downloaded by the any user. Private cloud need to provide much higher security for the users that the user stored files can be accessed by only that user. Unauthorized using of files must be detected and avoided in the private cloud.

2.1 Security Issue

The problem of providing security of confidential information remains a core 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, mis-configured services, faulty implementations, buggy code, and the creative construction of effective and sophisticated attacks not envisioned by the implementers of security procedures [9]. 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.

2.2 How OTFP works

The basic idea of OTFP is to avoid unauthorized access of file or documents stored in private cloud. Every user will be registered with cloud service provider. Each user will have a user login id and password for his access. Some old methods require only login and a key to access private cloud file. If any unauthorized user steels user id and password theft of documents is very easy. By using login id, password and access key file are enough to access file in private cloud storage. This paper proposes that private cloud provider has to register along with his personal valid Email id. This Email id is validated by a random generated 6 digit number code which will be sent as email to that registered Email id of the user.

Once the user Email id is registered with his user cloud account, it makes provision of alert service. Whoever logs in cloud with some login id and password, immediately an alert message will be sent to original user's registered Email id. If original user logged in, he can verify his login for validation so that, cloud data services will won't have any security risks.

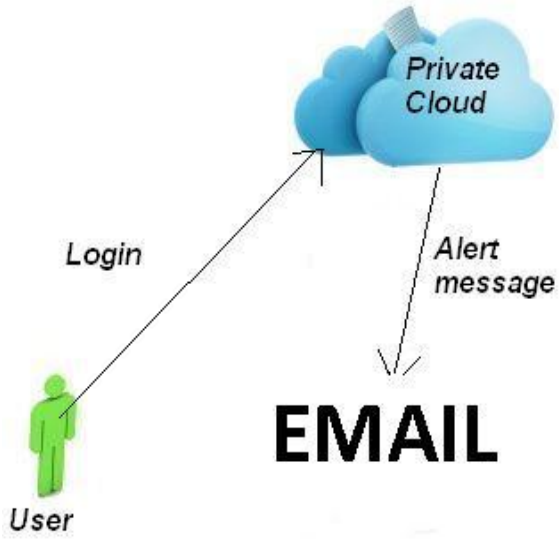

Figure 2: Alert message to user Email

Figure 2 explains how a user will get alert message from the cloud. If any unauthorized persons logs in immediately original user will receive an email so he can know that his account is being hacked he can block it and he can immediately change his login password so that his account can be secured. Figure2 shows proposed idea for securing files downloads.

When the user requests for the files or documents access for download, that file will not be downloaded immediately. A randomly generated 6 digit code will be sent as OTFP to registered Email id. If that 6 digit code entered by the user correctly then only file access is allowed if not file access is denied. Only authorized user can know the 6 digit random code which is sent by the cloud server. Every transaction of user download or login cloud service provider has to send and alert message to registered Email so that it can avoid attacks from hackers. If the user enters wrong 6 digit code for file access, then dummy file with duplicate data can be downloaded which is called as fogging of unauthorized user. The registered user should not use same password for his Email and File hosting account.

3. CONCLUSION

This paper proposes a new novel approach for securing the data from private cloud. One Time File Password is a service that protects unauthorized access of file hosting account and file downloading form the cloud. Unauthorized user account access and file access will be detected. An alert message and OTFP can be sent to user Email. So that theft attacks can be avoided in private cloud.

4. REFERENCES

[1] Cloud Security Alliance, "Top Threat to Cloud Computing V1.0," March 2010. Available:https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[2] M. Arrington, "In our inbox: Hundreds of con-fidential twitter documents," July 2009. [Online].Available:http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-of-confidential-twitter-documents/

[3] D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010. [On-line]. Available: http://venturebeat.com/2010/03/24/french-hacker-who-leaked-twitter-documents-to-techcrunch-is-busted/

[4] D. Danchev, "ZDNET: french hacker gains access to twitter's admin panel," April 2009. [Online].Available:http://www.zdnet.com/blog/security/french-hacker-gains-access-to-twitters-admin-panel/3292

[5] P. Allen, "Obama's Twitter password revealed after french hacker arrested for breaking into U.S. president's account," March 2010.[Online]. Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html

[6] 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.

[7] 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, 2010, pp. 1–8. [Online].Available:http://dl.acm.org/citation.cfm?id=1924931.1924934

[8] Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud.[Online].Available:http://ids.cs.columbia.edu/sites/default/files/Fog_Computing_Position_Paper_WRIT_2012.pdf

[9] J. Pepitone, "Dropbox's password nightmare highlights cloud risks," June 2011.