Securing Cloud Using Fog: A Review

Dipak Khadse[1], Akhilesh Amle[2], Sarang Charde[3], Shubham Deulkar[4], Pratik Patil[5]

[1,]Department of Computer Sci. & Engg,Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India
[2]Department of Computer Sci. & Engg,Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India
[3]Department of Computer Sci. & Engg,Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India
[4]Department of Computer Sci. & Engg,Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India
[5]Department of Computer Sci. & Engg,Priyadarshini Bhagwati College of Engineering, Nagpur, Maharashtra, India

---***---

Abstract - *Cloud computing is a platform which provides a way of accessing and storing personal as well as business information and also providing its users the resources through the internet. This type of computing invites data security challenges. Large amount of personal and professional data is stored in cloud which needs to be protected from data theft attacks, especially insider attacks. Cloud storage is used massively in industrial sectors. Security remains a major factor which needs to be focused on. We propose a different approach to secure data stored in cloud using User Behavior Profiling and Decoy Technology. We detect unusual data access patterns and monitor data access in cloud. When an unauthorized user activity is suspected and verified by using security questions, we deploy a disinformation attack by returning decoy information to the attacker. This ensures the security of the user's real data.*

***Key Words*: User Behavior Profiling, Decoy Technology.**

1.INTRODUCTION

Cloud storage is an strategical approach of networked enterprise storage where the data is stored in virtualized pools of storage. For the business enterprise outsourcing data and storing in cloud has become a natural option. Storing data on cloud has drawbacks which cannot be ignored [1]. Amplification of data theft is normal if the attacker is malicious insider which is considered as one of the top threats to cloud computing by the Cloud Security Alliance [2]. Cloud computing users are aware well-aware of this threat and the only option is to trust the service provider for protecting their data. Masqueraders acts as legitimate users after obtaining the credentials of authorized users when they try to gain access of Cloud. When the masqueraders logs in with the stolen credentials, he acts as the legitimate user with the same access rights as the real user [4].

One of the example being the credit card data breach at Marriot, Sheraton and other hotels. The company said information subject to potential theft by cyber criminals included names and numbers on consumers' debit or credit cards, security codes and card expiration dates.

The Twitter incident is one example of a data theft attack from the Cloud. Several Twitter corporate and personal documents were exfiltrated to technological website TechCrunch [5], [6], and customers' accounts, including the account of U.S. President Barack Obama, were illegally accessed [7], [8]. 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.

We propose a different approach to secure data stored in cloud known as Fogging. We use user behavior profiling and decoy information to secure the data stored in cloud. We deploy a disinformation attack against unauthorized users or to be precise an attack against malicious insiders using these two mechanisms we prevent them from discovering the original sensitive information.

1.1 User Behavior Profiling:

It is expected that access to a user's information in the Cloud will exhibit a normal means of access. User profiling is a well known technique that can be applied here to model how, when,and how much a user accesses their information in the Cloud. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. We monitor for abnormal search behaviors that exhibit deviations from the user baseline. According to our assumption,such deviations signal a potential masquerade attack.

This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. These simple user-specific features can serve to detect abnormal Cloud access based partially upon the scale and scope of data transferred.

1.2 Decoy Technology:

Decoy information, such as decoy documents, honeyfiles, honeypots, and various other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information and to 'poison' the thief's exfiltrated information. Serving decoys will confound and confuse an adversary into believing they have ex-filtrated useful information, when they have not. A masquerader, who is not familiar with the file system and its contents, is likely to access these decoy files, if he or she is in search for sensitive information, such as the bait information embedded in these decoy files This technology may be integrated with user behavior profiling technology to secure a user's information in the Cloud. Whenever abnormal access to a cloud service is noticed, decoy information may be returned by the Cloud and delivered in such a way as to appear completely legitimate and normal.

2. LITERATURE RIVIEW

Claycomb, W. R. (2012) [9] has characterized a hierarchy of administrators within cloud service providers and also gave examples of attacks from real insider threat cases. They discussed how cloud architecture let attackers to breach the security. They have also presented two additional cloud related insider risks: the insider who exploits a cloud related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local resource. They mentioned the key challenges faced by cloud providers and clients for securing their highly confidential data.

Salvatore J. Stoflio et al. [10] Proposed a new technique and named it as Fog computing. They implemented security by using decoy information technology. They discussed two methods, namely User behavior profiling and Decoy. In User behavior profiling they checked how, when and how much amount of information a user is accessing. They monitored their user's activity to check for any abnormality in the data access behavior of the user. The second technology is decoy in which information which is bogus or we can say fake such as honey files, honey pots, etc. are used to confuse the attacker or malicious intruder by depicting the information in such a way that it seems real.

Park, Y. Et al. (2012) [11] developed a technique that was a software decoy for securing cloud data using software. They proposed a software based decoy system that aims to deceive insiders, to detect the exfiltration of proprietary source code. The system builds a Java code which appears as valuable information to the attacker. Further static obfuscation technique is used to generate and transform original software.Bogus programs are synthesized by software that is automatically transformed from original source code, but designed to be dissimilar to the original.This deception technique confuses the insider and also obfuscation helps the secure data by hiding it and making bogus information for insider. Beacons are also injected into the bogus software to detect the exfiltration and to make an alert if the decoy software is touched, compiled or executed.

Kaufman L. et al. (2009) [12] has examined some security issues and the associated regulatory and legal concerns that have arisen as cloud computing. Interestingly,a major concern included in the Security Content Automation Protocol is the lack of interoperability between system level tools. By combining industry best practices with the oversight National Institute of Standards and Technology US and other entities are developing, we can effectively address cloud computing's future security needs. They also emphasize on the of providing data confidentiality which can impact the incident reporting.

Madsen.H and Albeanu. [13] presented the challenges faced by current computing paradigms and discussed how Fog computing platforms are feasible with cloud and are reliable for real life projects. Fog computing is mainly done for the need of the geographical distribution of resources instead of having a centralized one. A multitier architecture is followed in Fog computing platforms. In first tire there is machine to machine communication and the higher tiers deal with visualization and reporting. The higher tier is represented by the Cloud. They said that building Fog computing projects are challenging but there are algorithms and methodologies available that deal with reliability and ensure fault tolerance. With their help such real life projects are possible.

COMPARISION TABLE

Paper title	Techniques	Advantages
Improving Website's Performance using Edge Servers in Fog Computing Architecture	Minimizing HTTP requests, reducing the size of web objects and reorganizing the web page.	Concept of Fog Computing Architecture is used in such a way that various methods are combined with unique knowledge to improve the performance of rendering a web page.
Software decoys for insider threat	Developed a technique that was a software decoy for securing cloud data using software.	Discussed a technique that confuses the insider and also used obfuscation which helps to secure data by hiding it and making it bogus

		information for inside.
Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud	1-User Behavior Profiling 2-Decoy Information Technology	Monitor data and provides data security from malicious intruders and also helps in confusing the attacker about the real information.
Reliability in the Utility Computing Era: Towards Reliable Fog Computing	Three tier architecture for Fog Computing is discussed.	Provides the concept of Fog computing and its feasibility for real life projects.

3. CONCLUSION

The gradually increasing data theft attacks affects personal information of a user and has became an undeniable problem for cloud service providers for which fogging approach helps in understanding and monitoring a user behavior and in protecting user stored data. We hope that our work on Fog Computing will improve the defence against unauthorized information access and provide a layer of security for the user information stored in cloud.

REFERENCES

[1] Sayali Raje, Namrata Patil, Shital Mundhe, Ritika Mahajan “Cloud Security Using FogComputing” March 2014. Cloud Security Alliance, “Top Threat to Cloud Computing V1.0,” March 2010.
[2] Ben-Salem M., and Stolfo, Angelos D. Keromytis, “Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud,” IEEE symposium on security and privacy workshop (SPW) 2012.
[3]Ben-Salem M., and Stolfo, “Decoy Document Deployment for Effective Masquerade Attack Detection,” Computer Science Department, Columbia University, New York.
[4] M. Arrington, “In our inbox: Hundreds of con- fidential twitter documents,” July 2009.
[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] Claycomb, W. R., & Nicoll, A. “Insider Threats to Cloud Computing: Directions for New Research Challenges”, In Computer Software and Applications Conference (COMPSAC), IEEE 36th Annual, 2012, July, pp. 387-394.
[9] 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.
[10] Park, Y., & Stolfo, S. J. “Software decoys for insider threat”, In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012, May, (pp. 93-94).
[11] Kaufman, L. M. “Data security in the world of cloud computing”. Security & Privacy, IEEE, 2009, 7 (4), 61-64.
[12] 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.

BIOGRAPHIES

The author 1, Prof.D. B. Khadse received the B.E. Degree in Information Technology from Rashtrasant Tukadoji Maharaj University of Nagpur, India, in 2007. He has received Master ofEngineering (M.E.) Degree in Wireless Communication and Computing from G. H.Raisoni College of Engineering, Nagpur, Maharashtra.

The author 2,Mr.A.V.Amle student of final year,Department of Computer Science & Engineering, Priyadarshini Bhagwati College of Engineering,RTM Nagpur University.

The author 3, Mr.S.Charde studying in final year, Department of Computer Science & Engineering, Priyadrshini Bhagwati college of Engineering, RTM Nagpur University.

The author 4, Mr.S.Deulkar studying in final year, Department of Computer Science & Engineering, Priyadrshini Bhagwati college of Engineering, RTM Nagpur University.

The author 5, Mr.P.Patil studying in final year, Department of Computer Science & Engineering, Priyadrshini Bhagwati college of Engineering, RTM Nagpur University.