ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Minimizing Internal Data Theft in Cloud Through Disinformation Attacks

P.Jyothi[1], R.Anuradha[2], Dr.Y.Vijayalata[3]

Student, Department of CSE, GRIET, Hyderabad, India [1]

Student, Department of CSE, GRIET, Hyderabad, India [2]

Professor, Department of CSE, GRIET, Hyderabad, India [3]

Abstract- Cloud computing has changed the way computing takes place significantly. It is a new computing model which enables parties to make use of its services such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) in pay per use fashion. The users of cloud computing need not to indulge in huge capital investments as the resources are made available by cloud service providers. There are security challenges in cloud computing. One such challenge is data theft attacks. The existing mechanisms such as encryption are not able to present insider data theft attacks. Recently Stolfo et al. presented a mechanism to prevent insider data theft attacks using offensive decoy technology. In this paper we implement this technology by building a web based prototype that demonstrates the efficiency of the decoy technology. When the application suspects unauthorized access it throws challenges besides launching disinformation attack using decoy information. This prevents insider theft. The empirical results revealed that the mechanism is capable of providing security against insider data theft attacks.

Index terms-Encryption, decoy technology, decoy information

1. INTRODUCTION

Cloud computing has become a reality which paved the way for new model of computing. The users of cloud can outsource their data and also computations. With this facility made available without capital investment, the small and medium organizations opt for outshouting their data and computations to cloud. This gives the organizations many benefits besides operational efficiency. However, it brings security risks that are to be considered carefully. Very important concern is the insider data theft. When cloud service provider is unable to prevent insider data theft attacks, it is very important security concern. When malicious insiders who can steal data illegally throw challenges, the cloud service provider may not be able to prevent them. The Cloud SecurityAlliancehas considered this as a top threat [1]. Many users or customers of cloud computing are aware of this kind of threat. However, they have left their concern to cloud service provider believing that the cloud service provider takes care of it. There is lack of transparency, problem in data dynamics and security related problem like authorization, authentication, and audit controls etc.

Few years back there was a Twitter incident which is a best example for data theft attack from the cloud service provider. This incident exposed the security problems in cloud computing as it could make the customers of Twitter to lose their sensitive data and documents. The documents were ex-filtrated by TechCrunch [2], [3]. The President of United States Barak Obama was also a victim of the data theft attack. His files also were accessed illegally [4], [5]. The insider attacker had stolen Twitter's admin password and gained access to Twitters corporate documents. The incident caused significant damage to Twitter and its customer across the globe. This attack was reportedly made by an outsider. However, there is possibility to have internal attacks for data theft. In their work Rocha and Coriaexplored how to steal easy passwords through malicious insider of cloud service provider (CSP) [6]. They also demonstrated how to steal private keys and the confidential data which is saved in hard disk. Once credentials are stolen, an insider can gain access to customers' data illegally. There has been much research went on cloud computing security. Especially lot of research went on cloud computing and its storage problems. Much research is on preventing unauthorized access. However, the techniques fail when it comes to an insider data theft attack. Fully holomorphic encryption solution was proposed by Van Disk and Juels as a solution to such threats to protect data [7].

Recently Stolfo et al. [8] presented a novel mechanism for preventing insider data theft attack efficiently. This mechanism is based on offensive decoy technology. The technology is used to throw various challenges to users including questions besides launghing disinformation tracks.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

In this paper we implement the mechanism presented in [8] practically using a prototype application. Remainder of the paper is structured into some sections. Section II provides information about proposed mechanism. Section III provides information about the implementation. The section IV provides experimental results while section V concludes the paper.

2. PROPOSED SECURITY MECHANISM

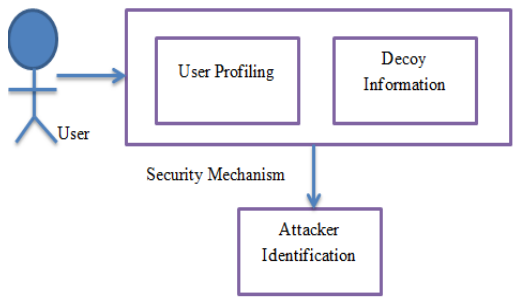

Fig 1. Security Mechanism

This section provides a security mechanism that can prevent insider data theft. This is achieved by launching disinformation attacks. This is preventive measure that ensures avoidance of insider data theft attacks. The proposed security mechanism makes use of two concepts known as user behavior profiling [9] and decoys. Users who access cloud to view their own data and also perform data dynamics are expected to have some specific patterns of usage. Such users are known as normal users. This normal behavior of users is profiled in the first phase. Then decoy information is kept in file system besides throwing varioussocietyequations. The insider theft attackers generally do not have the behavior of normal user. For this reason they are attracted to use decoy information. As the decoy information is not the real data there is no problem when hacker uses it or steals it. However, the navigational patterns of the malicious insider can be compared with the navigational patterns of genuine users. The abnormal behavior has to be suspected. The true user of cloud behaves normally and his activities match the general profile of any such users. When decoy information such as bogus information, honeypots, honey files and decoy documents are introduced into the file system, then the navigation of genuine users will be same as they try to use the legitimage content of their own. However, when adversaries try to use the system, they are definitely attracted towards decoy information as their job is to explore sensitive data and steal it for monetary and other benefits. The decoy technology is very useful as it deceives malicious insiders. When the decoy technology is used along with user profiles, it is possible to know the suspected behavior of users and that way it is possible to prevent insider data theft attacks. This kind of security has not yet implemented. In this paper, the prototype application makes use of the two approaches together to detect insider data theft attacks. When a rogue insider tries to use Cloud for data dynamics, he gets attracted to bogus information which appears sensitive and useful to hackers. This way the proposed application deceives malicious users to behave that way and avoid insider theft attack. The experimental results revealed that the combination of both the techniques such as user profile management and also the decoy technology could yield best results. The following section shows the implementation of the prototype application.

3. EXPERIMENTAL RESULTS

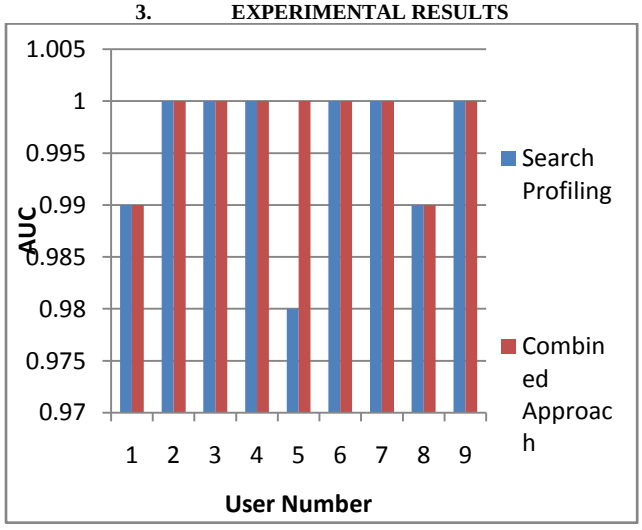

Fig.2. AUC Comparison by User Model for the Search Profiling

As can be shown in figure 6, it is represented horizontal axis is user number and vertical axis shows the AUC.

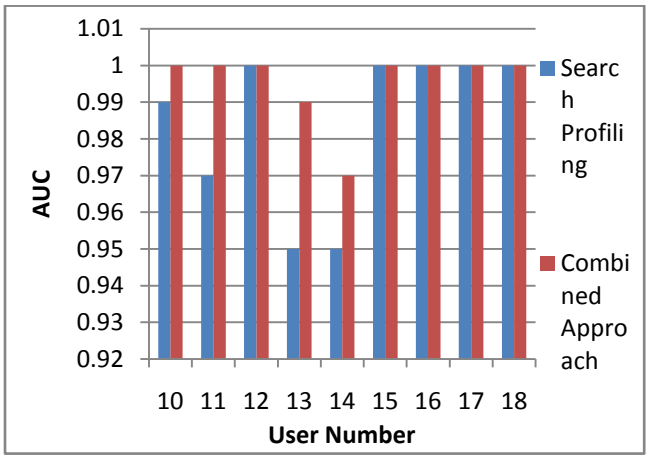

Fig.3. AUC Comparison by User Model for the Search Profiling and Integrated Approaches

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

As can be shown in figure 7, it is represented horizontal axis is user number, integrated approaches and vertical axis shows the AUC.

4. CONCLUSION AND FUTURE WORK

In this paper we implemented a prototype application that demonstrates proof of concept of a security mechanism presented by Stolfo et al. [8]. The security mechanism focuses on preventing insider data theft attacks. This is achieved by using two technologies together. They are known as user profile management and offensive decoy technology. These two approaches together could prevent insider data theft attacks. The user profile management ensures that the legitimate users' behavior and navigational patterns are recorded. The decoy technology allows the application to keep decoy information or bogus information in the file system to deceive insider data theft attackers. When malicious insiders enter into the cloud file system, they naturally get attracted to decoy information. This is because they do try for taking sensitive information that decoy mimics to have. Therefore the malicious insiders prefer navigating through decoy information which gives ample proof that the user who logged into the system is an attacker. The empirical results revealed that the proposed security mechanisms are effectively detecting malicious insiders who could commit data theft. This paper did not focus decoy information of pertaining to many domains such as banking, insurance, health care and so on. Moreover the user profile management can be improved further to have hierarchy of attributes of user data. These two will be our focus in future work. We would like to enhance the user profile management and use more decoy information from various domains for improving true positives of the fog computing.

REFERENCES

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

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

[3] D. Takahashi, "French hacker who leaked Twitter documents to TechCrunch is busted," March 2010. [Online]. Available: http://venturebeat.com/2010/03/24/french-hacker-wholeaked-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-totwitters-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] Salvatore J. Stolfo, Malek Ben Salem and Angelos D. Keromytis, "Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud". IEEE SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOP (SPW) YEAR 2012

[9] M. Ben-Salem and S. J. Stolfo, "Modeling user search-behavior for masquerade detection," in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1–20.

BIOGRAPHIES

Jyothi.P is student of GRIET College of Engineering and Technology, Hyderabad, AP, INDIA. She has received B.Tech Degree Computer Science and Eengineering and M.Tech Degree in Computer Science and Engineering. Her main research interest includes Cloud Computing, Databases and DWH.

Anuradha is student of GRIET College of Engineering and Technology, Hyderabad, AP, INDIA. She has received B.Tech Degree Computer Science and Engineering, M.Tech Degree in Computer Science and Engineering. Her main research interest includes Cloud Computing, Databases and DWH.

Dr. Y. VIJAYALATA is an academician with more than 17 years of teaching and research experience received M.Tech.(Computer Science) degree from Birla Institute of Technology, Ranchi, India and Ph.D. from JNTUH, Kukatpally, Hyderabad. Working as a Professor in Department of Computer Science and Engineering at GokarajuRangaraju Institute of Engineering and Technology(GRIET), Hyderabad.She is also the Chair, WIE-AG IEEE Hyderabad Section (2012-2013, 2013-2014). She was theVice-Chair for IEEE WIE Affinity Group, Hyderabad Section (2011-2012). She is the Branch Counselor for IEEE Student Branch at GRIET.