ATTACK RESISTANT MULTI LAYERED USER ACCOUNT RECOVERY TOOLKIT FOR CLOUD SERVICE PROVIDERS

Ms. R. ABINAYA*1 AND Dr. T. RAMAPRABHA2
1M.Phil Full Time Research Scholar, PG and Research Department of Computer Science Vivekanandha College of Arts and Sciences for Women [Autonomous], Tiruchengode,Tamilnadu,Namakkal-637 205,
2Professor, PG and Research Department of Computer Science Vivekanandha College of Arts and Sciences for Women [Autonomous], Tiruchengode,Tamilnadu,Namakkal-637 205.

Abstract- The Cloud Service Provider supports variety of services for the users. All the services are provided with User ID and password based authentication mechanism. The cloud security systems are constructed to handle the data and service level vulnerabilities. User account security is mainly focused to protect the user account recovery operations. Two security schemes are widely used to protect the account recovery tasks. They are Molecular Integration Simulation Toolkit (MIST) and Malachi schemes. The MIST security algorithm performs the user account recovery with predetermined questions and possible answer collections. The Malachi algorithm handles the account recovery with dynamic user queries and answers collected at the time of account generation. The attack resistant multi layered user account toolkit is build to secure the Cloud Service Providers. The account recovery operations are carried out with four layer analysis model. They are Question and Answer (QA) verification layer, Trustee based verification, One Time Password (OTP) based verification and Alternate account based verification methods. The QA based verification check outs the question and user reply information. The trustee based verification is carried out with the submission of the authentication code passed to the trustees. The OTP verification checks the password transferred to the user’s mobile. Finally the recovered account details are passed to the alternate user account.

Keywords- Cloud Web Services, Cloud Service Providers, Account Recovery, MIST, Malachi and Multi-way Authentication Scheme

I. INTRODUCTION

Web services today most commonly rely on passwords to authenticate users. Unfortunately, two serious issues in this paradigm are: users will inevitably forget their passwords and their passwords could be compromised and changed by attackers, which result in the failures to access their own accounts. Therefore, web services often provide users with backup authentication mechanisms to help users regain access to their accounts. Unfortunately, current widely used backup authentication mechanisms such as security questions and alternate email addresses are insecure or unreliable or both. Security questions are easily guessable and phished and users might forget their answers to the security questions. A previously registered alternate email address might expire upon the user’s change of school or job. For the above reasons, it is important to design a secure and reliable backup authentication mechanism.

The first sense of cloud services covers a wide range of resources that a service provider delivers to customers via the internet, which, in this context, has broadly become known as the cloud. Characteristics of cloud services include self-provisioning and elasticity; that is, customers can provision services on an on-demand basis and shut them down when no longer necessary. In addition, customers typically subscribe to cloud services, under a monthly billing arrangement, for example, rather than pay for software licenses and supporting server and network infrastructure upfront. In many transactions,
this approach makes a cloud-based technology an operational expense, rather than a capital expense. From a management standpoint, cloud-based technology lets organizations access software, storage, compute and other IT infrastructure elements without the burden of maintaining and upgrading them.

Facebook recently launched a new user authentication method called “social authentication” which tests the user's personal social knowledge. This idea is neither unique nor novel but Facebook's implementation is its first large-scale deployment. A user is presented with a series of photos of their friends and asked to select their name of a highlighted face from a multiple-choice list. The current system is used to authenticate user login attempts from abroad.

Facebook has invited security experts to find aws in the current system before a wider roll-out. If it were deployed for regular authorization and login systems and attacks were to be found subsequently, this could have wide repercussions for the many online merchants and websites which use Facebook to identify their customers, using the Facebook Connect OAuth 2.0 API. We therefore set out to find the best attacks we could on social authentication and this paper presents our results.

Social authentication is based on the intuition that the user can recognize her friends while a stranger cannot. At first glance, this seems rather promising. However, we argue here that it is not easy to achieve both security and usability: (1) the user's personal social knowledge is generally shared with people in her social circle; (2) photo-based social authentication methods are increasingly vulnerable to automatic attacks as face recognition and social tagging technologies develop; and (3) we face the same problems as in previous personal knowledge questions”.

Trustee-based social authentication has attracted increasing attentions and has been a promising backup authentication mechanism. Brainard et al. first proposed trustee-based social authentication and combined it with other authenticators as a two-factor authentication mechanism. Later, trustee-based social authentication was adapted to be a backup authenticator. In particular, Schechter et al. designed and built a prototype of trusted based social authentication system which was integrated into Microsoft’s Windows Live ID. Schechter et al. found that trustee-based social authentication is highly reliable. Moreover, Facebook announced its trustee-based social authentication system called Trusted Friends in October, 2011 and it was redesigned and improved to be Trusted Contacts in May, 2013.

Security of users is correlated in trustee-based social authentications, in contrast to traditional authenticators where security of users are independent. Specifically, a user’s security in trustee-based social authentications relies on the security of his or her trustees; if all trustees of a user are already compromised, then the attacker can also compromise him or her because the attacker can easily obtain the verification codes from the compromised trustees. The impact of this key difference has not been touched. Moreover, none of the existing work has studied the fundamental design problems such as how to select trustees for users so that the system is more secure and how to set the system parameters to balance between security and usability.

II. RELATED WORK

To address the growing problem of discovering malicious activities on social networks, researchers have started to propose different detection and mitigation approaches. In particular, several approaches to detect attacks and fake accounts in an OSN have been recently proposed. These are graph or behavior-based. Graph-based sybil detection schemes make assumptions about the OSN graph growth and structure. Based on these assumptions, researchers use various graph analysis techniques to develop algorithms for sybils detection, such as sybilGuard, sybil-Limit, sybilinfer and SumUp. Recent studies pointed out that these assumptions might not always hold. Indeed, it has been observed that sybils mix well into the rest of OSN graphs and that most of OSN graphs are not fast-mixing. These have implications in the proposed detection schemes, in that these may end up in false positive and false negative results: The best F-measure by removing one BF at a time [5]. Compared to graph-based sybil
defense techniques, our proposed risk assessment model is more flexible as it does not rely on the same assumptions, since we consider the activity patterns of sybils after they joined the OSN.

Most recent behavior-based approaches for the detection of anomalous users in OSNs exploit supervised learning techniques. As an example, in [8] to detect sybils, the proposed system trains a classifier by extracting four features, like: accepted incoming requests, accepted outgoing requests, invitation frequency and clustering coefficient. In [3], authors proposed an supervised approach to detect compromised account attack by using a small manually labeled dataset of legitimate and anomalous users. [9] used classifiers to detect spam and malware respectively. We have to note that the main issue of supervised learning is that they are not able to detect new attacker behaviors, since the classifier is trained based on the known behavioral patterns. Literature also offers approaches to detect anomalous users in OSNs that use unsupervised learning approaches. As an example, [11] used Principal Component Analysis to detect anomalous users in OSN. Their approach provides a framework for modeling user behavior in an OSN and leverage the user behavioral features to detect misbehavior. They detect anomalous users based on the number of likes per day. Although there is an issue that attackers can distribute their likes on several days to avoid detection and attacker with low level of activity cannot be detected because of intermixing between legitimate and anomalous behavior. In [12], the author proposed a combination of supervised and unsupervised techniques by analyzing the click stream behavioral of users in OSN in order to detect sybils.

Our analysis of attack behavior and characteristics demonstrates that most of the current unsupervised techniques are quite ad-hoc and complex. Some of these unsupervised behavior-based risk models suffer from high false negative and positive rates, due to the large variety and unpredictability of behaviors of both legitimate and malicious OSN users. In addition, existing attack defenses are designed to cope with just one type of attack [10]. Given the presence of several type of risky users in OSN, we believe a more comprehensive approach to effectively detect and defend against them is needed.

Similarly to this proposal, a risk measure for OSN users has been proposed. In [1] authors defined the local risk measure, that is, a measure computed only considering the similarity between two target users. In contrast, we propose a more general risk measure that takes into account behavioral patterns of a target user and compares them with the rest of network.

### III. CLOUD SERVICE SECURITY

Businesses that transition to cloud computing experience many benefits. Cloud Computing is a flexible way to allocate information technology resources such as storage, software infrastructures and bandwidth, out of a pool, enabling the business to consume power according to their needs [2]. Using a cloud based system provides a business the processing power to work efficiently through their peak data intensive processes, and save money by paying for only as much power as they need for less intensive processes by optimizing resources. Cloud users enjoy access to data stored on the cloud from any location with internet connectivity. Cloud Computing is revolutionizing the way data is stored and accessed. With Cloud Computing, a small business can access enterprise level computing without the high investment costs of allocating their own servers. Cloud Computing is cheaper than other computing models; zero maintenance cost is involved since the Cloud Service Provider is responsible for the availability of services, and clients are free from maintenance and management problems of the resource machines. Due to this feature, Cloud Computing is also known as Utility Computing, or ‘IT on Demand’.

Three important areas of research in Cloud Computing include security, performance and availability [4]. Security is by far the riskiest area of cloud computing. Cloud users experience a loss of security control over the cloud-hosted assets. It is the duty of the Cloud Service Provider to maintain the cloud infrastructure. This includes providing adequate security measures to protect cloud users’ private
data. Virtualization software, the prime technology used in Cloud Computing, and Cloud Computing itself contain many security weaknesses that affect data integrity and confidentiality. Some examples of these security issues are VMWare escape, hopping, mobility and diversity monitoring [6]. A good security algorithm presents a strategy to counter the vulnerabilities in a cloud system [7]. One of the most important aspects of improving security in the cloud is a strong security algorithm.

In the current computing world, where threats like the Sony Pictures Entertainment hack, the Sarah Palin email hack of 2008 and the recent Ashley Madison scandal are a constant reality, the importance of hardened security measures has become a dire concern. In order for a system to be protected from attacks, it is first necessary to identify the vulnerabilities. The algorithms covered in this paper focus mainly on eliminating the weak passwords and account recovery vulnerability that is common in today’s computing systems. Average users sometimes do not realize the importance of strong passwords and other inconvenient security measures and thus leave their accounts vulnerable to attacks in exchange for convenience. This means it is up to the system architects and developers to implement security measures that protect these users adequately, while giving the users the ease and convenience level they expect. This way the user is still protected without being overly inconvenienced by a security system.

The juxtaposition of a user’s convenience versus their level of protection is a huge factor in determining the best security algorithm to use in a system. The MIST security algorithm is an innovative solution that meets these needs. The MIST combines a simple, user friendly interface based approach to account recovery, while also incorporating highly user-specific questions. When the MIST algorithm is integrated in a system, account recovery becomes far more secure.

IV. ISSUES ON CLOUD SECURITY SERVICES

The cloud security systems are constructed to handle the data and service level vulnerabilities. User account security is mainly focused to protect the user account recovery operations.

Two security schemes are widely used to protect the account recovery tasks. They are Molecular Integration Simulation Toolkit (MIST) and Malachi schemes.

The MIST security algorithm performs the user account recovery with predetermined questions and possible answer collections. The Malachi algorithm handles the account recovery with dynamic user queries and answers.

In the Malachi scheme security questions and answers are collected during the account creation process. Malachi scheme performs the user verification at the time of each login attempt and account recovery process. The following issues are discovered from the current cloud security services.

- The system can be vulnerable to compromised attacks
- The user accounts can be easily broken with profile history details
- Temporal feature based authentication is not supported
- Single authority based recovery models
The attack resistant multi layered user account recovery toolkit is build to secure the Cloud Service Providers. The MIST and Malachi schemes are enhanced with multi layered verification models. The account recovery operations are carried out with four layer analysis model. They are Question and Answer (QA) ,Trustee, One Time Password (OTP) and Alternate account based verification methods. The QA based verification check outs the question and user reply information. The trustee based verification is carried out with the submission of the authentication code passed to the trustees. The OTP verification checks the password transferred to the user’s mobile. The recovered account details are passed to the alternate user account. The Cloud Service Provider (CSP) and client applications are constructed to share services. The MIST and Malachi schemes are constructed with question and answer verification tasks. Multiple levels of verification is performed in the multi layered verification model. The system is divided into five major modules. They are Cloud Service Provider, Cloud Client, Recovery with MIST, Recovery with Malachi and Multi Layered Verification Scheme.

The Cloud Service Provider (CSP) supports resource and service sharing through the Internet. User accounts and profile information are maintained under the Cloud Service Provider (CSP). The cloud services are provided with reference to the results of the user authentication process. User account recovery information and settings are maintained under the Cloud Service Provider. Cryptography and digital signature techniques are used to secure the cloud data values. The symmetric cryptography and
asymmetric cryptography methods are used in the cloud service provider environment. The cloud client is built to access the resources and services provided by the Cloud Service Provider. The cloud user authentication process is carried out through the cloud user gateway environment. The user can monitor and modify the account profile and account settings. The user accounts are protected with multi layered account recovery mechanism. All the client data values are uploaded with security and privacy. Encryption and decryption schemes are used to protect the data values.

The Molecular Integration Simulation Toolkit (MIST) is adapted for the user account recovery process in the cloud based services. User selected question and associated answer collections are used in the MIST security algorithm for user account recovery. Multiple question and answers (QA) are verified in the recovery process. The recovery controller verifies all the authentication tokens for the account recovery process. The MIST scheme is applied for the password recovery process. The Malachi scheme is adapted for the user account recovery and login attempts. Dynamic query based verification is initiated in the Malachi scheme. The question and answers are collected during the user account generation process. The login verification is initiated with reference to the user choice model. The Malachi scheme is also used for the password recovery process on user accounts.

The attack resistant multi layered user account recovery toolkit is build with multi layered verification technique. The Question and Answer (QA) based verification process checks the user assigned questions with its answers. The One Time Password (OTP) scheme verifies the dynamic authentication code is used to the user mobile. Trustee and alternate account based verification are also called in the multi layered verification model. A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has as well as something a person knows such as a PIN. The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

VI. EXPERIMENTAL ANALYSIS

The cloud services are build with question and answer based authentication mechanism for user account recovery operations. The MIST, Malachi and Multi-layered User Account Recovery (MUAR) schemes are used in the user account recovery process. The multi layered user account recovery toolkit is build with question and answer based verification, One Time Password (OTP) based verification, trustee based verification and alternate account based verification methods. The system is tested with two performance parameters.

They are Recall Ratio Analysis and Strength measures. The One Time Passord is transferred to the user registered devices such as mobile phone. The recover password is transferred to the alternate mail account.
The recall ratio is estimated with the account recovery rate details. The recall ratio analysis between MIST, Malachi and Multi-layered User Account Recovery (MUAR) scheme are shown in figure 6.1. The Malachi scheme increases the recall ratio 15% than MIST scheme. The Multi-layered User Account Recovery (MUAR) scheme increases the recall rate 10% than the Malachi scheme. The user account protection and recovery level is measured with the strength measure. The strength analysis
between MIST, Malachi and Multi-layered User Account Recovery (MUAR) scheme are shown in figure 6.2. The Malachi scheme increases the Strength Analysis 10% than MIST scheme. The Multi-layered User Account Recovery (MUAR) scheme increases the Strength Analysis 20% than the Malachi scheme.

VII. CONCLUSION

The cloud resources are shared by the Cloud Service Providers (CSP). The missed user passwords are fetched with the user account recovery methods. The Molecular Integration Simulation Toolkit and Malachi schemes are used for the account recovery process. Attack resistant multi layered user account recovery toolkit is build with Question and Answer, trustee and external verification methods. The Cloud Service Providers are secured with the multi layered account verification method. External verification is carried out with trustee and alternate accounts. The verification process is initiated for login and recovery operations. Brute force and password guessing attacks are controlled by the system.

REFERENCES

[1] Cuneyt Gurcan Akcora, Barbara Carminati and Elena Ferrari. Privacy in social networks how risky is your social graph? In Data Engineering (ICDE), 2012 IEEE 28th International Conference on, 2012.
[2] R. Chalse, A. Selokar and A. Katara, “A New Technique of Data Integrity for Analysis of the Cloud Computing Security”, 5th Annual Conference on Computational Intelligence, 2013.
[3] Manuel Egele, Gianluca Stringhini, Christopher Kruegel and Giovanni Vigna. Compa- detecting compromised accounts on social networks. In NDSS, 2013.
[4] Z. Xin, L. Song-qing and L. Nai-wen, “Research on Cloud Computing Data Security Model Based on Multi-Dimension”, International Symposium on Information Technology 2012.
[5] Yazan Boshmaf, Dionysios Logothetis, Georgos Siganos, Jorge Ler’ia, Jose Lorenzo, Matei Ripeanu and Konstantin Beznosov. Integro: Leveraging victim prediction for robust fake account detection in osns. In Proc. of NDSS, 2015.
[6] M. N. Omar, M. Salleh and M. Bakhtiari, 2014 International Symposium on Biometrics and Security Technologies (ISBAST), “Biometric Encryption to Enhance Confidentiality in Cloud Computing”, 2014.
[7] D. Devkota, P. Ghimire, J. Burris and I. Alkadi, “Comparison of Security Algorithms in Cloud Computing”, IEEE, 2015.
[8] Zhi Yang, Christo Wilson, Xiao Wang, Tingting Gao, Ben Y Zhao and Yafei Dai. Uncovering social network sybils in the wild. ACM Transactions on Knowledge Discovery from Data (TKDD), 2014.
[9] Md Sazzadur Rahman, Ting-Kai Huang, Harsha V Madhyastha and Michalis Faloutsos. Efficient and scalable socware detection in online social networks. In USENIX Security Symposium, 2012.
[10] Naeimeh Laleh, Barbara Carminati and Elena Ferrari, “Risk Assessment in Social Networks based on User Anomalous Behaviours”, IEEE Transactions on Dependable and Secure Computing, 2016.
[11] Bimal Viswanath, M Ahmad Bashir, Mark Crovella, Saikat Guha, MSR India, Krishna P Gummadi, Balachander Krishnamurthy and Alan Mislove. Towards detecting anomalous user behavior in online social networks. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security), 2014.
[12] Gang Wang, Tristan Konolige, Christo Wilson, Xiao Wang, Haitao Zheng and Ben Y Zhao. You are how you click-clickstream analysis for sybil detection. In USENIX Security, pages 241–256, 2013.