Cloud Computing Authentication using Cancellable Biometrics

Krishnaraj Madhavjee Sunjiv Soyjaudah, Gianeswar Ramsawock, Muhammad Yaasir Khodabacchus
Faculty of Engineering
University of Mauritius
Reduit, Mauritius

***Abstract*— Cloud computing has increasingly been a hot topic in the recent years and has achieved maturity. However security concerns are the hindrance to user acceptance of cloud computing systems. User authentication among them requires a high-guaranteed security since all protections rely on the mechanism. As such in recent years biometric technologies are becoming one of the key foundations of a wide range of secure identification and personal verification solutions. In a cloud computing environment, since control over security diminishes as data move dynamically, they present some problems related to the management of biometric data. To overcome this problems, in this paper we propose to use a cancellable biometric authentication system. In this concept a distorted biometric image, derived from the original, is used for authentication. Additionally a data hiding technique is used to embed demographic information in the biometric image. As a result a robust authentication is created by which the original biometric image is not exposed.**

Keywords—cloud computing; biometrics; security; privacy; authentication

I. INTRODUCTION

Cloud computing is a way of delivering applications over the Internet. Instead of installing and maintaining software, they can simply be accessed via the Internet, freeing from complex software and hardware management [1]. On the other hand, the migration of the applications on the cloud raised concerns regarding the privacy of sensitive data associated with the consumers. The providers manage access to the application, including security, availability, and performance. While using these applications, consumers provide the service providers with sensitive data such as identification number and credit card information in order to have access to these online services. Existing laws and legislation call for cloud computing service providers to implement various security measures depending on the nature of the information. Nevertheless, consumers cannot confirm that a provider of a service conform to the actual legislation and also safeguard their digital identity [2]. In addition the sophistication in the tools used by malicious users is constantly on the increase, the data within the cloud is with increasing risk of an attack. All protections rely remarkably on the mechanism of user authenticating [3]. Access is by far the weakest link in the security chain, since it represents the point of contact between the clouds and between the users and the application they need to operate with [4].

Fig 1. Access

Consequently, there is an immediate requirement of robust authentication systems to ensure that the information can be used solely by simply genuine, approved consumers. This username/password safety symbol is utilized by simply the majority of providers to help authenticate buyers, which leaves the consumer prone to attacks such as phishing.

In wake of that issue a biometric-based authentication by Bennet and Arumugaperumal [5] was presented. Authenticating the user based on biometrics is more reliable than the more traditional means of password authentication since biometric authentication is unique and slow intrusive [6]. However, biometrics raises several privacy concerns. A biometric is permanently associated with a user and cannot be changed. Hence, if a biometric identifier is compromised, it is lost forever and possibly for every application where the biometric is used [7]. Moreover, if the same biometric is used in multiple applications, a user can potentially be tracked from one application to the next by cross-matching biometric databases. In this paper we outline the inherent strengths of biometrics-based authentication, identify the weak links in systems employing biometrics-based authentication, and present a new solution for eliminating some of these weak links.

II. STATE OF THE ART

Cloud computing is the latest extension of an evolution in distributed computing that takes advantage of technology advances. The cloud's roots date back to early mainframe processing, when users connected to a shared computing resource through terminals to solve their computing needs [8]. The particular introduction of faster and cheaper microprocessors, memories and storage brought computing into the client-server model, which grouped sets of users into

978-1-4673-5943-6/13/$31.00 ©2013 IEEE

networks sharing computing power on decentralized asset servers. As bandwidth became more ubiquitous, speedier, and less costly, these networks interconnected to form the Internet. IT departments typically provisioned their data centers in house, protected inside a firewall.

Eventually, corporations took benefit of greater throughputs to re-examine the necessity pertaining to monolithic onsite data centers. Accessing servers essentially by having a web browser screen shown considerable rewards in software and hardware maintenance. Software vendors began capitalizing on the concept that a scaled data centre could also deliver remote content to customers almost immediately at a reduced cost, giving rise to on-demand Software-as-as-Service.

Cloud computing has revolutionized the world of information technology. Today's developed virtualization platforms make it possible for a whole new style of speedy, on-demand, low-cost, al-a-carte computing.

A. Types of Cloud

Cloud computing can be classified as Private, Public and Hybrid. Based on the service that the cloud is offering, Trend Micro [9] has identified several different configurations of cloud computing. Each approach offers its own strengths, risks, and level of control that is provided to the cloud consumer.

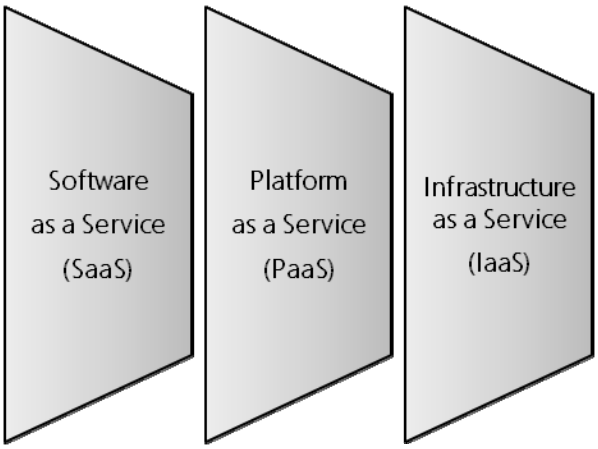

Fig 2. Types of cloud services

1) Software as a Service

In an October 2009 publication [10], Peter Mell and Tim Grance of the U.S. National Institutes of Standards & Technology (NIST) defined Software as a Service (SaaS) as the capability for a consumer to use the provider's applications running on a cloud infrastructure. It is understood that the cloud users do not manage the cloud infrastructure and platform where the application runs.

2) Platform as a Service

Platform as a Service (PaaS) provides the cloud consumer with the capability to deploy applications onto the cloud platform using programming languages and tools that are supported by the cloud provider.

3) Infrastructure as a Service

Infrastructure as a Service (IaaS) gives the cloud user the most control of the three types of clouds. The cloud consumer has the ability to provision processing, storage, networks, and other fundamental computing resources, where the consumer is able to deploy and run arbitrary software such as operating systems and applications.

B. Data Security and Privacy

The public nature associated with cloud computing poses significant implications to data privacy and confidentiality. Cloud data is often stored in plain text, and few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly. In fact, a recent report by the Cloud Security Alliance [11] lists data loss and leakage as one of top security concerns in the cloud. Loose data security practices also harm on a personal degree. Lost or stolen healthcare documents, credit card numbers or bank information may cause emotional along with fiscal ruin, this repercussions might get several years to mend. Sensitive data stored within cloud environments must be safeguarded to protect its owners and subjects alike.

Due to the intriguing nature of security and privacy in cloud computing, traditional authentication based on password cannot meet the projected dimension. Biometrics which is an emerging set of technologies promise an effective solution. Biometric data are independent and different from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information [12].

III. BIOMETRICS

The word biometrics is derived from the Greek words bios (meaning life) and metron (meaning measurement), so biometrics is in essence, the measure of life [13]. As the level of security breaches and fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric recognition techniques have been used in forensic applications for over 100 years. They have helped criminal investigations, identified disaster victims, and helped to locate missing children [14]. Biometric systems can spare investigators the time-consuming process of sorting through thousands of files by hand. Also forged or stolen identification cards are a common security problem all over the world. According to the United Kingdom's Identity and Passport Service [15], over 290,000 U.K. passports are lost or stolen each year. Some international airports are adopting iris, fingerprint, or face recognition systems to prevent individuals from entering a country using false credentials.

Biometrics in the field of information technology is a concept of identifying information system users and protecting such systems against intruders. The system is actually

powerful taking into consideration some greats benefits about biometrics, although regrettably a biometrics system is not fully secured.

A. *Vulnerable points*

Eight possible places of attacks have been identified in a biometrics-based authentication system by Vacca [16]:

1- Presenting a possible reproduction of the template as input to the system
2- Resubmitting previously stored digitised template.
3- The feature extractor is attacked by a Trojan Horse so that it produces feature sets preselected by the intruder.
4- The features extracted from the input signal are replaced with a different, fraudulent feature set.
5- The matcher is attacked and corrupted so that it produces preselected match scores
6- The database of stored templates can be attacked with one or more templates modified to authorise a fraudulent individual or denying service to a legitimate person.
7- The stored templates are sent to the matcher through a communication channel. The data travelling through the channel can be intercepted and modified
8- The final match can be overridden rendering the authentication system disabled.

In the following section a new schema is proposed to overcome some of the weaknesses listed above.

IV. PROPOSED SCHEMA

The proposed schema involves namely two steps; data hiding and transformation.

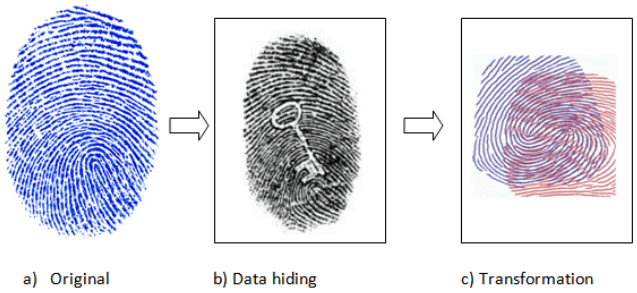

Fig 3. The solution

A. *Data Hiding*

Inspired by the ancient Greece [17], data-hiding technique is utilized to enhance security by means of embedding additional information directly in the biometric image. This strategy can be determined because of the desire to build biometric authentication programs which can be safe against replay attacks. In achieving this, an alternative verification sequence can be given for each request.

A particular string is blended in with the biometric image before transmission. When the image is received by the server it is decompressed and the image is checked for the presence of the correct one-time verification string. The method proposed here hides such messages with minimal impact on the appearance of the decompressed image. Moreover, the message is not concealed in a fixed location but is, instead, deposited in different places based on the structure of the image itself.

Unless the disguised facts can be removed with a reasonable level of assurance, the biometric image may become invalid. One-time verification is a form of strong authentication, and offer more effective protection. It prevents different forms of identity theft by ensuring that a combination cannot be used a second time.

B. *Cancellable Biometrics*

Ratha [18] from IBM Research states that one of the properties that make biometrics so attractive for authentication purpose is their invariance over time but it is also one of its liabilities. When a credit card number is jeopardized, the issuing bank can just assign the customer a new credit card number. When the biometric data are compromised, replacement is not possible.

In order to alleviate this problem, the concept of cancellable biometrics is introduced. It consists of an intentional, repeatable distortion of a biometric signal based on a chosen transform. The biometric signal is distorted in the same fashion at each presentation, for enrolment and for every authentication.

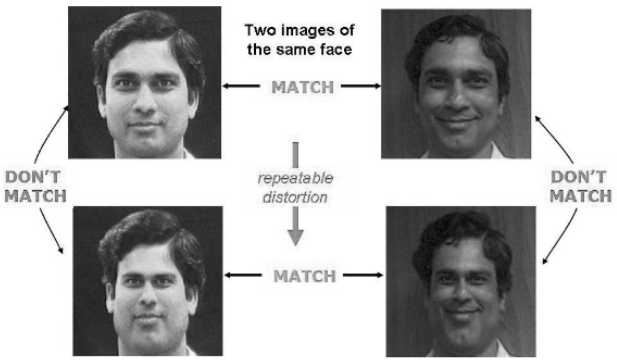

Fig 4. Example of a distortion

With this strategy, every instance of enrolment can use an alternative transform thus rendering cross-matching impossible. Moreover, in the event that one variant of the transformed biometric data is compromised, then the transform function can simply be changed to create a new variant for re-enrolment. In general, the distortion transforms are selected to be noninvertible. So even if the transform function is known and the resulting transformed biometric data are known, the original biometrics cannot be recovered. Cancellable biometrics ensures that template protection is achieved at the feature level with the assistance of the

auxiliary data/non-invertible transforms. Subsequently a notable enhancement is attained in terms of privacy.

V. CONCLUSION

Biometrics-based authentication has many usability advantages over traditional systems such as passwords. Specifically, users can never lose their biometrics, and the biometric signal is difficult to steal or forge. Yet a biometric system is vulnerable when attacked by determined hackers. Eight points of vulnerability have been highlighted and methods of how to overcome them have been discussed. Data-hiding techniques will be used against replay attacks by secretly embedding information in the biometric image. Furthermore, once a set of biometric data has been compromised, it is compromised forever. Therefore to address the issue, an intentional distortion is applied to the biometric image. As a result, the distorted biometric image can be cancelled. Security and privacy is enhanced due to the fact that different distortions can be used for different purposes and the original biometrics are never stored or revealed to the authentication server.

REFERENCES

[1] G. Kulkarni , J. Gambhi , R. Palwe, "Cloud Computing-Software as Service," International Journal of Computer Trends and Technology, vol.2, no.2, pp.178, 2011.

[2] B. Bhargava , N. Singh , A. Sinclair, "Privacy in Cloud Computing Through Identity Management," Dept. Elect. And Comput. Eng., Purdue Univ., pp.1.

[3] A.A. Yassin, H. Jin, A. Ibrahim, W. Qiang, D. Zou, "Efficient Password-based Two Factors Authentication in Cloud Computing," International Journal of Security and Its Applications, vol. 6, no. 2, pp.143, 2012.

[4] Stonesoft, "Combining Modern Authentication Needs with Identity and Access Management," Starting Managed Security Services with the Stonesoft, pp.4, 2012.

[5] D. Bennet, S. Arumugaperumal, "Fingerprint Authentication Scheme for Cloud Security," International Journal of Engineering Technology and Computer Application, vol. 1, pp.1, 2012.

[6] H. Vallabhu, R.V. Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution," International Journal of Soft Computing and Engineering, vol. 2, no. 4, pp.163, 2012.

[7] J.R Vacca, "Identity Theft Future Solutions and Technologies" in *Identity Theft*, United State of America: Pearson Education, 2003, pp.27.

[8] Trend Micro, "Addressing Data Security Challenges in the Cloud. The Need for Cloud Computing Security," pp.3, 2010.

[9] Trend Micro Cloud Protection, "Security for Your Unique Cloud Infrastructure," Data Center and Cloud Security, pp.4, 2011.

[10] P. Mell, T. Grance, "The NIST Definition of Cloud Computing," Computer Security, pp.2, 2011.

[11] Cloud Security Alliance, "Guidance for Identity and Access Management," pp.6, 2010.

[12] V.K. Pachghare, *Authentication. Cryptography And Information Security.* India: PHI Learning Private Limited, 2009, pp.168.

[13] M. Schatten , M. Bača, M. Čubrilo, "Towards a General Definition of Biometric Systems," International Journal of Computer Science Issues, vol. 2, pp.1, 2009.

[14] Biometrics Research Group. (2009). *Biometrics Application* [Online]. Available: http://biometrics.cse.msu.edu/info/.

[15] International Currency Exchange. (2009). *Passport Assist one stop for foreign currency and passport protection* [Online]. Available: https://www.iceplc.com/press/2009/stay-cool-with-ice-if-passport-is-lost-or-stolen.html.

[16] J.R. Vacca, *Biometric Technologies and Verification Systems*. United State of America: Butterworth-Heinemann, 2007, pp. 293.

[17] A. Kumar, K.M. Pooja, "Steganography- A Data Hiding Technique," International Journal of Computer Applications, vol. 9, no. 7, pp.19, 2010

[18] N. Ratha, J. Connell, R.M. Bolle, S.t Chikkerur. "Cancelable Biometrics: A Case Study in Fingerprints." *18th International Conference on Pattern Recognition*., 2006, pp.1.