REVIEW: AUTHENTICATION IN CLOUD COMPUTING

Kapila Purohit(PG Student)
Department of Computer Science
Arni School of Technology, Arni University
Kathgarh (H.P.), India
Email id: peetambari.kapila@gmail.com

Assistant Professor Mr. Anurag Rana
Department of Computer Science
Arni School Of Technology, Arni University
Kathgarh (H.P.), India
Email id: anuragrana.anu@gmail.com

Abstract— Cloud computing is becoming popular. This is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle. It is a general term for the delivery of hosted services over the internet. Cloud offers various services that not only stored but can also be shared among multiple users. However, the security of cloud computing is always center of attention of various potential cloud customers, and big obstacle for its widespread applications. Many approaches for authentication in cloud services have been proposed. They are insecure, intricate or highly expensive. In this Paper, to assist people to understand the basics concept of cloud computing and put in some efforts to deal with one of the major security issues that is security of cloud computing, we surveyed the existing popular security models of cloud computing and summarized the mains threats of cloud computing.

Keywords— Cloud Computing, Authentication, Security.

Introduction (*Heading 1*)

Recently, cloud computing has gained a considerable acceptance as a promising model from both business and academic communities. It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The Cloud Computing paradigm is now emerging as one of the new technologies, with companies of all sizes accessing the Cloud. As cost efficiency, unlimited storage, backup and recovery, automatic software integration, easy access to information stand out as advantages, security issues stand out as the major disadvantages of this new technology. Cloud computing comprises of three typical service standards that include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). It instances can be operated and exploited according to four different deployment models such as private cloud, public cloud, hybrid cloud and community cloud. Cloud computing delivers various services over web such as information storage and infrastructure. Cloud service providers provide applications and computing resources through internet, in which they can be accessed anywhere using web browsers, desktops and mobile applications. Cloud computing delivers software as a service through Internet. Cloud computing is a web based model in which more than one system is connected in the distributed environment for enabling suitable, instant network access to a shared computing resources.

Cloud computing allows tenants to store programs or documents stored individually in large-scale computer to which can be accessed anytime and anywhere, and to perform necessary works through various terminal units including PCs or mobile phones. In cloud computing environment tenants borrows and uses cloud resources as required and pays the expenses as used. Most large sized organizations have enough investment strength and high technical skills to build private cloud for the reason of security. However, small and medium-sized organizations lack capital compared with large-sized organizations and so they tend to use public cloud with lower initial capital and operation costs compared with private cloud. Additionally, the cloud computing technology comes with several problems and various security issues. So far, various schemes have been proposed, to provide adequate security to cloud computing. However, these existing security schemes decrease security measures. The major issue consists of multi-tenancy, packet transmission, storing and encrypting user's data, application security, cloud integrity and security related to third-party. Moreover, the openness nature of internet has many security flaws. Therefore, attackers can misuse these

flaws to disturb various services using various kinds of attacks and threats.

In Cloud security, authentication is the most important factor. In cloud computing still there is a need for well-defined authentication mechanisms. One of the first steps toward securing an IT system is to verify the identity of its users. The process of verifying a user's identity is typically referred to as user identification and authentication. Authentication is generally referred to as a mechanism that establishes the validity of the claimed identity of the individual. There is basically four kinds of authentication methods:

a. Something an individual KNOWS (e.g. password, Personal ID)
b. Something an individual POSSESSES (e.g. a token or card)
c. Something an individual IS (e.g. fingerprint or voice pattern)
d. Something an individual DOES (e.g. history of internet usage)

2 Authentication Trends in Cloud Computing

In general authentication is the act of validating someone as authentic and claims they made are true. In cloud computing, validation is generally done using the login username and password. Knowledge of the password is adopted to ensure that the tenant is authentic. Each tenant registers first or gets registered by someone else on cloud server and using an assigned or self-stated password. During each successive use, the tenant must know and use the already declared password. A number of researchers are working to find good or strong authentication methods for cloud computing. A number of authentication methods are running for work. In this, a critical review of various research works is carried out. To identify the review and new approaches are divided into different categories. The weakness of this system is that passwords can often be stolen, unintentionally revealed or forgotten. There are a couple of possible authentication attacks. There are common authentication methods:

A. Password and PIN Based Authentication

Using password (a secret word or string of characters that is used for user authentication) or Personal Identification Number (PIN which is a secret numeric password and is typically used in ATMs) to login is the most common knowledge-based authentication method. A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access.

B. SMS Based Authentication

SMS is used as a delivery channel for a one-time password (OTP) generated by an information system. There are two types of one-time passwords, a challenge-response password which responds with a challenge value after receiving a user identifier and a password list which makes use of lists of passwords which are sequentially used by the person to access a system. User receives a password through the message in the cell phone, and enters the password to complete the authentication. This SMS-based authentication method is used in the login process of Internet banking for authenticating the user's login. 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 (or similar) 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.

C. Symmetric Key Authentication

In symmetric key authentication, user shares a secret, unique key with an authentication server. The user may be asked to send a randomly generated message (the challenge) encrypted by the secret key to the authentication server. If the server can found the match for received encrypted message (the response) using its shared secret key, the user is authenticated and server authorizes user's access to the system. Key authentication is used to solve the problem of authenticating the keys of the person (say "person B") to whom some other person ("person A") is talking to or trying to talk to. In other words, it is the process of assuring that the key of "person A" held by "person B" does in fact belong to "person A" and vice versa. This is usually done after the keys have been shared among the two sides over some secure channel, although some of the algorithms share the keys at the time of authentication also.

D. Biometric Authentication

The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure).Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. Computer science, biometrics to be specific, is used as a form of identification. Biometric systems allow identification of individuals based on behavioral or physiological characteristics [2].Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. Biometric systems can be used in two different modes. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in

this case the biometric data obtained from the user is compared to the user's data already stored in the database. Identification (also called search) occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all .

E. Multi-factor Authentication

A more secure scheme is the multi-factor authentication which does not only verify the username/password pair, but also needs second factor such as biometric authentication. However, the feasibility of second factor authentication is limited by the deployment complexity, high cost. MFA technique uses combination of something you have, something you know as well as something you are to supply stronger authentication method. It is stronger user identification techniques. In fact, the trust of authenticity increases exponentially when more factors are involved in the verification process. For example, ATM transaction requires multifactor authentication, something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A type of multi-factor authentication using fingerprints and user-specific random projection. The proposed method used the concept of random projection and fixed length fingerprint feature extraction to generate revocable and privacy preserving templates that yield high authentication accuracy. This feature vector is known as finger code.

F. Mobile Trusted Module

Trusted Computing Group (TCG) introduced a set of specifications to measure, store and report hardware and software integrity through a hardware root-of-trust, which are the Trusted Platform Module (TPM) and Mobile Trusted Module (MTM). MTM is a security factor for employ in mobile devices. Unlike Trusted Platform Module (TPM) that is for PCs, MTM is employed in mobile devices. However, for high levels of protection and isolation, an MTM could be implemented as a slightly modified TPM. MTM checks all software and applications each time the underlying platform starts due to increase the security of mobile devices. Therefore, the MTM guarantees the integrity of a mobile platform. It has very constraints such as circuit area, as well as available power. Therefore, a MTM needs the spatially-optimized architecture and design method. TPM provides trusted information on the internal state of the system and stores cryptographic keys and identities. It is accessed by software using a well-defined command set. Through this command set, the TPM provides cryptographic functionality such as encrypting, signing, key generation and random number generation. It could also store a limited amount of information in nonvolatile memory.

3 Conclusion

Authentication method is main factor of preserving security and privacy of each communication in cloud computing. With large variety of applications security is also an important issue in cloud computing. But authentication in cloud users will gaining more interest in cloud computing. Main mechanism of authentication is that "Who is the legal user" and "Is the user really who he claims himself to be". We have discussed numerous methods of authentication in this paper.

Acknowledgment

This research paper was partially supported by Mr. Anurag Rana (our guide). We thank our colleagues from Arni University who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretation or conclusion of this paper.

References

[1] Yashpalsingh Jadeja , Kirit Modi "*Cloud Computing – Concepts , Architectures and Challenges"* , 2012 International Conference on Computing , Electronic and Electrical Technology [ICCEET] , 978-1-4673-0210-9/12/$31.00 2012 IEEE

[2] Tharam Dillon , Chen Wu and Elizabeth Chang, "*Cloud Computing : Issues and Challenges"* , 2010 IEEE International Conference on Advanced Information Networking and Applications , 1550-442X/10$26.00@ 2010 IEEE

[3] Shobha Rajak , Ashok Verma ,"*Secure Data Storage in the Cloud Using Digital Signature Mechanism"* , ISSN : 2278-1323 , International Journal of Advanced Research in Computer Engineering and Technology Volume 1 , Issue 4, June 2012

[4] Shikha Choksi, "Comparative *Study on Authentication Schemes For Cloud Computing*", 2014 IJEDR, Volume 2, Issue 2, ISSN: 2321 – 9939.

[5] Mahoush Babaeizadeh, Majid Bakhtiari and Alwuhayd Muteb Mohammed, "*Authentication Methods in Cloud Computing: A Survey*", Research Journal of Applied Sciences, Engineering and Technology, 2015.

[6] Lisa J.Sotto , Bridget C. Treacy , and Melinda L , Mc Lellan , "*Privacy and Data Security Risks in Cloud Computing*", Reproduced with Permission From Electronic Commerce and Law Report, ISECLR 186. (Feb 3, 2010)