Volume 7, Issue 2, February 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on User Authentication Techniques and Attack Taxonomy in Cloud Computing

[1]Madhuri Dhange*, [2]Rajani Sajjan, [3]Vijay Ghorpade
[1, 2] Department of Computer Science & Engineering, VVPIET, Solapur, Maharashtra, India
[3]D.Y. Patil College of Engineering & Technology, Kolhapur, Maharashtra, India

DOI: 10.23956/ijarcsse/V7I2/0122

Abstract*— Cloud computing is an extended environment of information technology services that offers unlimited computing services to improve productivity and operational efficiency. It supports resource sharing and multi-tenancy with reduced capital and operational expenditure. So nowadays, the private enterprises, government organizations, educational institutional are adopting cloud services for their work. As ease of use and low-cost benefits are two main features of cloud computing, security and trust are two main issues related to cloud services. In recent years, a lot of research on cloud security has been carried out and many more techniques and methods are proposed to overcome cloud security issues. One such security measure we are focusing here is user authentication. This paper identifies different authentication attacks and techniques approached to improve authentication in Cloud.

Keywords*—Cloud Computing, Cloud Security Issues, Cloud Attack Taxonomy, Cloud Authentication.

I. INTRODUCTION

Cloud computing is an extended mechanism of most Internet based services. It offers unlimited computing services to improve productivity and operational efficiency. It supports resource sharing and multi-tenancy with reduced capital and operational expenditure. Cloud enables its users to increase their proficiency in services vigorously without investing in new infrastructure, without training new personnel, without licensing new software etc. So nowadays, the private enterprises, government organizations, educational institutional are adopting cloud services for their work. The U.S. National Institute of Standards and Technology (NIST) defined cloud computing as," Cloud computing is a delivery model that enables convenient instant network access to a pool of shared configurable computing resources that can be quickly provisioned and released ". Cloud model supports availability of resources and has many characteristics such as on-demand self-service, distributed network access, resource pooling, measured service and rapid elasticity [1].

Basically cloud computing offers three types of service to its users categorised as software, platform and infrastructure. These services known as, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). And it provides four deployment models such as Private cloud, Public cloud, Hybrid cloud and Community cloud which closely resembles to Internet deployment models [1].

Cloud computing technology allows cloud users to remotely access shared resources which resides on cloud servers using web services via the Internet. Hence the cloud resident resources are viable to the security threats which are related to Internet and web services. The resources should be accessible only to users who has authority. It point's outs requirement of deriving a secure, user authentication mechanism for the cloud environment. Authentication encompasses the process of ensuring a person identity to whom he or she claims to be. The cloud service providers have to take responsibility to tackle the issues faced by user authentication mechanisms which is carried out before providing access to shared resources. However, to achieve the full benefits of cloud services, the cloud service providers need to tackle with various security concerns such as data security, trust and privacy etc. [2].

The cloud service providers have access to the customer's data stored in cloud which again leads to privacy concerns. Cloud does not allow customers to monitor their own privacy information, even customer is unaware about his data location on cloud. So there is a lack of transparency in cloud though SLA's guarantees privacy of sensitive data. Subscribing to several cloud services means multiple copies of user credentials exists, which is yet another security issue. For every cloud service accessed by the customer, needs to exchange his/her authentication information. This redundancy may lead to a corruption of the authentication mechanism. Hence, a fool proof user authentication mechanism is a paramount requirement of the cloud environment to prevent illegal access to cloud resources or services [3], [4].

The paper is organized as follows: Section 2 discusses a possible various types of authentication attack taxonomy for cloud. Many of these attacks are inherited from web services as cloud services uses web services as a tool for delivering its services, so those threats are applicable to cloud as well. Section 3 reviews various authentication techniques proposed for cloud environment to enhance the security of cloud computing. Section 4 concludes the survey work.

II. CLOUD AUTHENTICATION ATTACK TAXONOMY

Any authentication mechanism should provide high security, easy to use interface and support user mobility. In web based services or cloud services, customers prefer to access resources from different locations and different devices such as desktop, laptop, PDA, smart phones, cell phones etc. So it needs significant requirement of security to resources. The wide range of user requirements introduces wide range of attack vectors in cloud that makes cloud resource security threats. Cloud service providers need to ensure that only authorised user can access their services and this points out to the requirement of a strong user authentication mechanism. But there exists several attacks that can create loop holes in the authentication process. It is a big challenge to identify the most secure authentication mechanism with high user acceptability in the cloud environment. Thus an in-depth knowledge of attacks on authenticity and corresponding prevention techniques are required to develop a fool proof authentication mechanism for cloud environment. This section describes some possible authentication attacks in cloud computing. The Fig.1. shows a pictorial representation of taxonomy of authentication attacks.

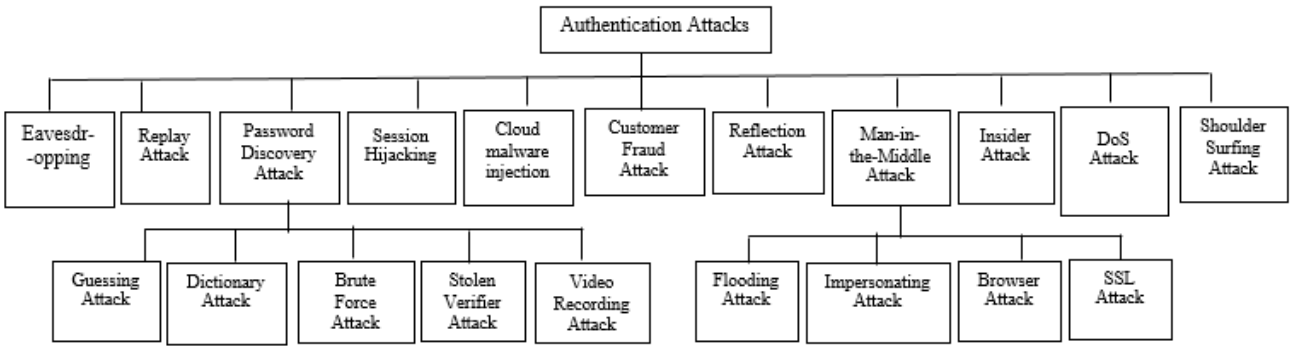

Fig. 1 Authentication Attacks Taxonomy in Cloud Computing

A. Eavesdropping Attack

Eavesdropping attack launched by listening to the communication channel established between two authorized users. A traffic eavesdropper can passively intercept data transferred in cloud by loading a bit of code on a cloud server or listens to data moving between a cloud consumer and provider and makes an illegal copy of message [5], [6], [7].The attacker can use this illegally gathered data to get valid credentials of an authorized user which helps to launch impersonating attack.

Performing data encryption and a signature attachment to the same before transmission over the communication channel can help the destination to ensure the integrity and authenticity of data. Implementing privacy-enhancing protocols which reduce the requirement of transmission of identity credentials between cloud service user and the verifier, will discourage the illegal activity of eavesdroppers.

B. Replay Attack

In a capture-replay attack the authentication message contains same authentication tokens which are previously exchanged between an authorized users. Here, attacker sniffs authentication credentials and replay the authentication process [7]. To handle replay attack, which includes identity spoofing, a mechanism needed to ensure that something in the message changes each time. Many protocols use time stamps or randomly generated nonce values to resist replay attack. It enables the verifier to check freshness or authenticity of message. The usage of time stamps demands synchronization of timing at both end. But this may not be feasible in a distributed cloud environment. Hence randomly generated nonce is unique value generated for each session are more preferable in a Cloud environment. So the attacker will fail to launch a replay attack as captured message contains an old nonce value.

C. Password Discovery Attack

To retrieve passwords stored in computer system or transmitted over communication channel, attackers adopt several mechanisms to launch this attack. It includes Password guessing attack, Dictionary attack, stolen verifier attack, Brute-force attack, Video recording attack. In Brute-force attack, attacker tries all possible combinations of letters, numbers and alphanumeric characters until the attacker get the correct password. Brute force attack usually carried out using automated methods which demands a lot of computing power and time, to be successful. In stolen verifier attack, attacker performs this attack by accessing the password table stored at the verifier end.

D. Session Hijacking Attack

If the Session ID issued to the authenticated users is not secured properly, then it can be used for spoofing identity. Encrypting the communication channel can avoid this type of Session hijacking attack [7].

E. Cloud Malware Injection

The attack intentions is injecting a malicious services (SaaS/PaaS) or virtual machine instance (IaaS), which appears as valid service instances running in the cloud environment. For instance, adversary launches the attack by making its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS) and injects it

into the cloud. If it becomes successful, then the cloud system consider it as valid instance for the particular service which can results into a hazard.

To tackle this attack, calculate and store a hash value of the original service instance's image file and compare with that of all new service instance images whenever required. If a modification is done to a valid service instance, then the hash value will be modified which indicates the presence of an attacker.

F. Customer Fraud Attack

In this type of attack, the user intentionally compromises its authentication credentials for illegal activity. In a cloud scenario this attack can be tackled by using one time passwords or randomly generated nonce values in authentication protocols. These values which are unique to each session are securely communicated to the customer by the verifier.

G. Reflection Attack

Reflection attack is performed on mutual authentication schemes wherein the attacker tricks the target into revealing the secret to its own challenge. This attack performed by creating parallel session which is launched by an unauthorized user to establish a valid session with the server.

In a cloud scenario, this kind of attack can be minimized by keeping track of the sessions, secrets used for each session as well as limiting the number of established session. Again ensuring that the communication messages exchanged between the user and the cloud server during the authentication process are not symmetrical in nature can help mitigate reflection and parallel session attacks.

H. Man-in-the-Middle (MITM) Attack

Here the attacker interrupts the communication channel established between authorised users and alters the communication between client and server without their knowledge [7]. MITM attacks includes Flooding attack, Browser attack, Impersonating attack, SSL attack.

In flooding attack, the adversary floods the bogus requests to keep the computational resources busy so that other customers' requests get starve in cloud environment. This attack can be controlled by data transfer throttling, fool proof authentication mechanisms and mechanisms that filter out bogus requests.

In browser attack, adversary steals data by sabotaging the signature and encryption during the transformation of SOAP (Simple Object Authentication Protocol) messages in between the web browser and web server, causing the browser to consider the adversary as a authorized user and process all requests, communicating with web server [16]. The counter measure to this attack is to enable WS-Security to web browsers. WS-Security permits web browsers to use XML encryption to provide end-to-end encryption in SOAP messages which prevents sniffing of messages.

In impersonating attack, the adversary pretends to be a legitimate server or user and appeals a valid entity to disclose the authenticating credentials. Phishing attacks is type of impersonation attack ,here the users are made to believe that they are communicating with valid server by creating a web page that look similar to the valid server page. This attack can be avoided in a cloud environment by using two-factor or multi factor authentication mechanisms that trust on personally identifiable information (PII) in addition to passwords [8].

SSL (Secure Socket Layer) layer is a fundamental security mechanism that encrypts data transmitted between client and server. SSL provides an authenticated environment for cloud services by verifying the identities of the communication parties [9]. It consist of stripping attack and sniffing attack.

I. Insider Attack

Insider attack is launched by someone inside the security perimeter who is purposely compromising the security. An insider can be a current or former employee, contractor or business partner of an organization who is intentionally misuse his right to access the sensitive resources of the organization which negatively affects confidentiality, integrity or availability organizations information systems [10]. In a cloud environment an insider can be a fraud cloud provider administrator or the employees in organization that exploits cloud weaknesses for unauthorized access or the insider who uses cloud resources to carry out attacks against the company's local IT infrastructure. In order to prevent and detect malicious insider activity, cloud provider must have noticeable security access control policies, enable auditing of user actions, support the segregation of duties, and principle the least privilege for privileged users.

J. DoS Attack

The main objective of DoS (Denial of Service) attack is to overload the target machine with bogus service requests to prevent it from responding to legitimate requests. Unable to handle all the service requests on its own, it delegates the work load to other similar service instances which ultimately leads to flooding attacks. As cloud supports resource pooling so it is more vulnerable to DoS attacks. This attack can be controlled to a certain extent by data transfer throttling which deliberately regulates the amount of data transferred per unit time among the communicating entities.

K. Shoulder Sniffing Attack

The attacker gains knowledge about security credentials by observing credentials entry via the keyboard, spy camera. Even a partially successful shoulder surfing attack can be dangerous when used with other security threat combinations. In cloud scenario it can be avoided by using secure two factor authentication and out of band authentication mechanisms.

III. CLOUD AUTHENTICATION TECHNIQUES

User authentication in cloud environment is as significant concern, because it gives assurances that somebody accesses or shares data with legitimate person and that only legitimate users can have access to data or applications [11]. Authentication possesses some form of "proof of identity". In cloud environment, there is increasing demand for suitable authentication technique to access shared information via the Internet through cloud service provider. Therefore, several mechanisms are used to authenticate users in cloud environment. From last decade, much development has taken place in authentication field, numerous authentication models are proposed by researchers. There are basically three kinds of authentication credentials based on – something an individual Knows, something an individual Possesses, and something an individual Is. This section reviews various techniques that are typically employed for authentication such as Username and password, Biometric authentication, Multi-factor Authentication, Mobile Trusted Module (MTM), Public Key Infrastructure (PKI), and Single Sign On (SSO).

A. Username and Password Authentication

In this method of authentication, user should provide valid username and password to login the system and can get access to services. It is comprehensively supposed that username and password is not very safe authentication mechanism as it can be compromised easily by attacker, so it is difficult to ensure the request is from legitimate owner. Moreover, commonly users choose easy, short passwords to remember but it can be easily guessed which causes increase in risk to security. Even the best password can be stolen by dictionary and brute force attacks. Increasing password strength is a solution to avoid these attacks. Numerous protocols proposed which allows users to use a single password to authenticate identity in multiple services securely. These protocols help to guard users against cross-site attack, dictionary attack, phishing and malware [12]. The graphical password authentication also proposed to improve security of cloud services. It encompasses an identification algorithm by using username and images as a password [13].

B. Multi-factor Authentication(MFA)

Conventional password authentication method does not ensure enough security for cloud computing environment to the most modern means of attacks. So the secure Multi-factor Authentication (MFA) technique used which verifies more than two factors. For instance, verifies username/password as first factor, along with second factor biometric authentication. However, the feasibility of second factor authentication is limited by its deployment complexity, high cost etc. MFA technique uses combination of something you have, something you know as well as something you are, for stronger authentication method. In fact, the trust of authenticity increases exponentially when more factors are involved in the verification process. For instance, ATM transaction requires a smart card which consist a security token and a PIN no. for authentication. Researchers proposed many authentication models based on MFA. One of the model provides a mechanism that can closely integrate with the traditional authentication systems. The framework is verified by Cloud Access Management (CAM) system which authenticates the user based on multiple factors such as Arithmetic captcha, OTP (One Time Password), IMEI no. of smart phone [14].

C. Biometric Authentication

Biometric techniques depend on the user's personal physical and behavioural attributes. Bio-metric authentications are receiving more popularity in the critical security fields such as in finance. The common bio-metric scheme includes fingerprints, palm prints, hand geometry, retina recognition, voice recognition, face recognition. Each biometric recognition scheme can be analysed on the basis of several factors such as uniqueness, time, acceptability, number of false alarms etc. The main weakness of these schemes is the requirement of a special scanning device to authenticate users, which is not applicable for remote based users. It is a static authentication system where identity of the user is verified at the start of the session, for instance using a fingerprint to get access to a computer or using an iris scan to get access to security room [15].

D. Mobile Trusted Module(MTM)

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 which is based on mobile devices and TPM on personal computers. However, for high levels of protection and isolation, an MTM could be implemented as a slightly modified TPM. To increase the security of mobile devices, MTM checks each time all software and applications installed when underlying platform starts. So MTM guarantees the integrity of a mobile platform. It has some constraints such as circuit area, available power. Therefore, a MTM needs the spatially-optimized architecture and design method [16]. MTM is mainly applied to authentication terminals from telecommunication channel to accomplished security functions such as, hash functions, signature schemes, and asymmetric encryption. However nowadays MTM authentication methods are considered with Subscriber Identity Module (SIM) because of generalization of smart phones. It ensures reliability of a mobile platform [16].

E. Public Key Infrastructure(PKI)

PKI is based on the secret key and it mainly supports the deployment of conventional asymmetric cryptographic algorithms, such as RSA. It uses a private key (secrete key) to prove the user's identity. PKI has been used in the design

of security protocols such as Secure Socket Layer (SSL/TLS) and Secure Electronic Transaction (SET) with the main aim is to provide authentication. The success of PKI depends on controlling access to private keys. PKI ensure data confidentiality, data integrity, non-repudiation, strong authentication, as well as authorization. It is used with combination of other authentication technology to provide robust security to cloud services. PKI also used for several cryptography applications such as encryption, key agreement, digital signature etc. [17]. The main advantage of PKI is to provide authentication users in distributed systems like as cloud computing, mobile cloud computing and wireless sensor network.

F. Single Sign On(SSO)

Single Sign on (SSO) is an identity management system where user access the multiple independent software system in such a way that user logs in a system and gains access to confined systems without being prompted to re-login in each application [18]. This method helps to decrease the risk for the administrators to direct users substantively. It enhances user's efficiency by preventing the user to remember numerous passwords. It minimizes time the user applies on typing different passwords to login.

IV. CONCLUSIONS

Cloud computing is an extended mechanism of most Internet based services. It offers unlimited computing services to improve productivity and operational efficiency. It offers a wide range of benefits to small and medium enterprises. But security, privacy and trust are the major concerns which prevents the mass adoption of cloud. A cloud environment that provides numerous services and hosts multiple resources can be secured only by providing authorized access. Hence a strong user authentication mechanism designed for cloud to protect cloud from various possible malicious authentication attacks. This work surveys possible authentication attacks and authentication techniques used in cloud environment.

REFERENCES

[1] Mell. P, Grance T., *The NIST definition of cloud computing,* version 15 technical report. Computer and Information Science, vol. 53(6), pp.1-10, 2009.

[2] Vaquero L., Rodero-Merino L., Caceres J., and Lindner M., *A break in the clouds toward a cloud definition.*, ACM sigcomm Computer communication review, vol. 39, pp.50-55, 2009.

[3] W.Liu, *Research on Cloud Computing Security Problem and Strategy*, in Proc. IEEE 2nd Int. Conference on Consumer Electronics, Communications and Networks, pp. 1216-1219, 2012.

[4] H. Takabi, J.B.D Joshi, G.Ahn, *SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments*, in Proc. IEEE 34th Annual Computer Software and Application Conference Workshops, pp. 393-398, 2010.

[5] Larry Hardesty, *Thwarting the Cleverest attack*, [online]. Available: mit.edu/newsoffice/2012,thwarting-eavesdropping-data-0501.html

[6] Maventek, *Cloud Security Consulting* [online] Available : www.maventek.com/services/Cloud-security-consulting

[7]]Kazi Zunnurhain and Susan V. Vrbsky,, *Security Attacks and Solutions in Clouds*, [Online] Available: http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.

[8] M.Misbahuddin, *Secure Image Based Multi-Factor Authentication (SIMFA): A Novel approach for Web Based Services*, Ph.D Thesis, Jawaharlal Nehru Technological University, [Online], Available: http://shodhganga.inflibnet.ac.in/handle/10603/3473.

[9] Abel Wike, *SSL Encryption – A Protocol that Authenticate Cloud Computing*, [Online] Available: comluv.com/ssl-encryption-a-protocol-that-authenticateCloud-computing.

[10] D.Cappelli, A.Moore, and R.Trzeciak, *The CERT Guide to Insider Threats: How to prevent, Detect and Respond to Information Technology Crimes (Theft, Sabotage , Fraud)* . SEI series in Software Engineering. Addison-Wesley Professional, 2012.

[11] Jivanadham, L.B., A.K.M. Islam, Y. Katayama, S. Komaki and S. Baharun, Cloud Cognitive Authenticator (CCA): A public cloud computing authentication mechanism. Proceeding of International Conference on Informatics, Electronics and Vision (ICIEV, 2013), pp. 1-6, 2013.

[12] Acar, T., M. Belenkly and A.Kupcu, *Single password authentication,* IACR Cryptology ePrint Archive, pp. 167, 2013.

[13] Gurav, S.M., L.S. Gawade, P.K. Rane and N.R. Khochare, *Graphical password authentication: Cloud securing scheme,* Proceeding of IEEE Electronic Systems, Signal Processing and Computing Technologies (ICESC, 2014), pp. 479-483, 2014.

[14] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain, *Multi-factor Authentication Framework for Cloud Computing*, Fifth International Conference on Computational Intelligence, Modeling and Simulation, IEEE, 2013.

[15] Jiang, X.C. and J.D. Zheng, *An indirect fingerprint authentication scheme in cloud computing*. Applied Mechanics and Material, ISSN : 1662-7482, vol. 484, pp. 986-990, 2014.

[16] Kim, M., H. Ju, Y. Kim, J. Park and Y. Park, *Design and implementation of mobile trusted module for trusted mobile computing*. IEEE T. Consum. Electr., vol. 56(1), pp. 134-140, 2010.

[17] Akyildiz, E.,M. Ashraf, *An Overview of trace based public key cryptography over finite fields*, J. Comput. Appl. Math.,vol:259, pp:599-621.

[18] Revar, A.G. and M.D. Bhavsar, *Securing user authentication using single sign-on in cloud computing*, Proceeding of International Conference on Engineering (NUiCONE), pp: 1-4, 2011.

