ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

A Survey of Cloud Authentication Attacks and Solution Approaches

B.Sumitra*[1], C.R. Pethuru[2], M.Misbahuddin[3]

[1]Research Scholar, Dept. of Computer Science, Christ University, Bangalore, India

[2]Infrastructure Architect, IBM Cloud Global Center of Excellence, IBM India Pvt. Ltd., Bangalore, India

[3]Senior Technical Officer, C-DAC, Electronic-City, Bangalore, India

*Corresponding Author

ABSTRACT: Cloud computing is an evolving computing paradigm that offers great potential to improve productivity and operational efficiency. This recently developed technology supports resource sharing and multi-tenancy which in turn contributes towards reduced capital and operational expenditure. While cost and ease of use are the main benefits of cloud computing, trust and security are the two top concerns of users of cloud services. The providers of this fast growing technology need to address many issues related to virtualization distributed computing, application security, identity management, access control and authentication. However, strong user authentication that restricts illegal access to the service providing servers is the paramount requirement for securing cloud environment. In this regard, the paper focuses on identifying the various authentication attacks in cloud environment. An attempt has been made to understand the root cause of the authentication attacks and propose possible mitigation measures in a cloud environment.

KEYWORDS: Cloud Computing, Security Issues, Classification, Authentication Attacks, Counter measures.

1. INTRODUCTION

Cloud computing is a new generation technology that offers on-demand, network access to a shared pool of configurable computing resources on a pay per use basis. This new computing paradigm differs from other similar computing technologies in that, the cloud computing services follow a self-service model. Cloud computing offers software, platform and infrastructure over the Internet and this constitutes the three flavors of cloud viz., Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). This computing model enables the cloud users to increase their capacity and capability dynamically without investing in new infrastructure, training new personnel, licensing new software etc. [1].

Cloud computing technology enables users to remotely access shared resources stored in cloud servers using web services via the Internet. Hence the cloud resident resources are viable to the security threats applicable to Internet and web services. The fact that the resources should be accessible only to legitimate user's points out to the requirement of deriving a secure, user authentication mechanism for the cloud environment. Authentication involves the process of ensuring that a person who presents a set of credentials is whom he or she claims to be. The cloud service providers need to tackle the issues faced by user authentication mechanisms carried out prior to providing access to the shared resources.

The architectural features of cloud such as Multi-tenancy and Virtualization allow the users to achieve better operating costs and be very agile by facilitating fast acquisition of services and resources on a need basis. However, to achieve the full benefits of cloud, the service providers need to tackle the security concerns raised by the fast growing cloud consumers. Among the various security concerns, data security, trust and privacy are the major ones that make potential customers think multiple times before adopting cloud services. In a survey conducted by International Data Corporation (IDC), to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

understand challenges of Cloud computing, 87.5 % of the masses belonging to varied levels starting from IT executives to CEOs have said that security is the top most challenge to be dealt with in every cloud service [2]. Amongst the various threats faced by the different cloud services, security threat is considered to be of high risk [3] and hence the cloud service providers need to consider security as a serious issue to be addressed immediately for the whole hearted adoption of cloud services. These threats can be thwarted in an application by the introduction of some suitable elements based on the goals of information security paradigm. The goals include Confidentiality, Data-Integrity, Authenticity, Authorization, Non-Repudiation, Availability, Audit and Control [4, 5, 6].

The fact that cloud service providers have access to the customer's data stored in the cloud leads to privacy issues. There is a lack of transparency in cloud that allows customers to monitor their own Privacy information, though SLA's guarantee privacy of sensitive data. Subscribing to multiple cloud services means multiple copies of user credentials, which is yet another security issue. For every cloud service accessed by the customer, he needs to exchange his authentication information and this redundancy may lead to an exploitation of the authentication mechanism. Also different cloud service providers use different authentication mechanisms which can be a security challenge for the customers. Hence, a fool proof user authentication mechanism is a paramount requirement of the cloud environment to prevent illegal access to cloud provided resources.

II. ORGANIZATION OF THE PAPER

The rest of the paper is organized as follows: Section 3 discusses a few works done by researchers in the area of cloud Security and authentication. Section 4 examines the various categories of authentication attacks on cloud. Many of these attacks are applicable to web services and since cloud services often uses web services as a tool for delivering its services, these threats are applicable to cloud as well. The presented work describes the various authentication attacks from the perspective of cloud and discusses possible countermeasures. Section 5 is reserved for a brief discussion of the work done by the researchers and for concluding the work.

III. RELATED WORK

In recent years, many researchers have proposed multifarious approaches to investigating security issues of cloud computing. Meiko Jensen et al. [7] consider the technical security issues arising from the usage of cloud services and the underlying technologies used to build these cross-domain inter-connected collaborations. This work concentrates more on web services related security issues and concentrates less on authentication factor. Hassan Takabi et al., [8] have identified cloud computing as an unstoppable force because of its potential benefits. The authors highlight the need to have appropriate mechanisms to handle the security and privacy risks in cloud. The work discusses the security challenges including user authentication, access control, policy integration, trust management and service management and proposes a comprehensive security framework for cloud computing . Hsin-Yi Tsai et al [9] in their work explores the security issues in different service delivery models from the perspective of Virtualization.

S.Subashini and V.Kavitha [1] surveyed the security risks faced by the cloud service delivery models and suggests a security framework that provides data security by storing and accessing data based on meta-data information. B. Sumitra and M. Misbahuddin [10] has surveyed and categorized the security threats applicable to cloud environment. The work is a general classification of attacks and does not delve deep into authentication issues. Rohit Bhadauria et al. [11] investigated the security threats such as SQL injection flaws, cross-site scripting, insecure storage etc. as applicable to cloud environment. But the focus is on the various layers of the network such as Network level and Application level. R.C.William et al. [12] discusses the insider threats in cloud computing. The authors consider the insiders from three different perspectives and the possible impact of each insider on cloud Security. But this work concentrates only on a specific category of authentication attack on cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Although there is a considerable amount of ongoing research for identifying the security loop holes in cloud there is a need to consider the specific challenges faced by various architectural components of cloud. Also the technologies used by cloud for delivering its services raises various security issues, which needs to be identified and addressed. The authentication mechanism used by cloud service providers contributes a lot towards the enhancement of security features since cloud hosts a huge number of shared and sensitive resources. Drafting an authentication framework, which can address the security concerns related to authentication, requires a clear understanding of all possible authentication attacks on cloud. Hence identifying the various categories and subcategories of authentication attacks, attack scenarios and possible mitigation techniques becomes the motivation for this work.

IV. AUTHENTICATION ATTACKS IN CLOUD

Research studies reveal that any authentication mechanism related to web applications and cloud should provide high security, easy to use interface and support user mobility. The customers prefer to access their applications from different locations and different devices such as desktop, laptop, PDA, smart phones, cell phones etc. Those needs pose significant requirements to the security of applications. The broad range of user requirements introduces wide range of attack vectors in the cloud that makes the security of cloud applications a thought provoking matter. Cloud service providers need to ensure that only legitimate user are accessing their services and this points out to the requirement of a strong user authentication mechanism. But there exists numerous attacks that can create loop holes in the authentication mechanism and hence identifying the most secure authentication mechanism with high user acceptability is a big challenge in the cloud environment. Thus an in-depth idea of attacks on authenticity and corresponding prevention techniques are required to draft a fool proof authentication mechanism for cloud environment. Figure 1 gives a pictorial representation of the attacks on authenticity and in the sections that follows, a detailed description of the attacks and the possible solutions are given.

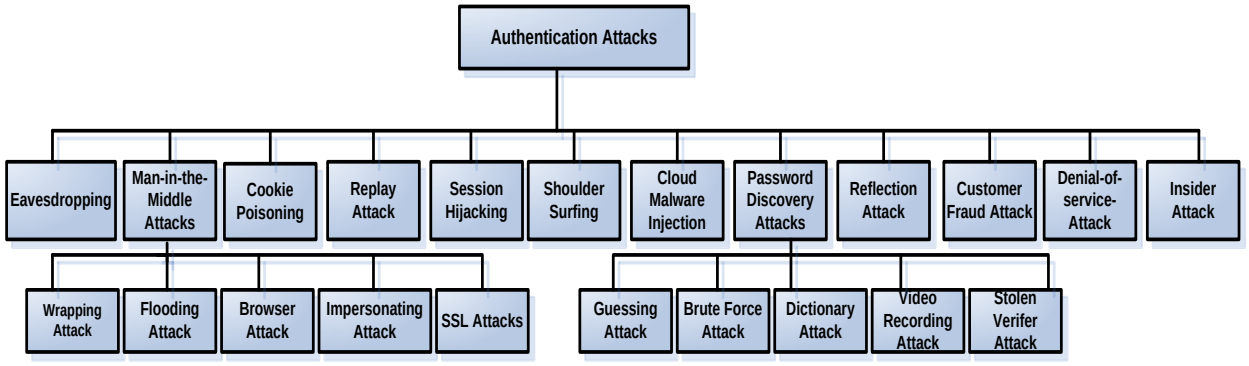

Fig 1: Classification of Authentication Attacks in the Cloud Environment

4.1 Eavesdropping: Eavesdropping involves the act of listening to the communication channel established between two authorized users. In a cloud environment, a traffic eavesdropper passively intercepts the data transferred within a cloud by loading a bit of code on a cloud server [13] or listens to data moving from a cloud consumer to provider and makes an unauthorized copy of the message [14].The attacker can use the illegally gathered information to get valid credentials of an authorized user which can be user to launch impersonating attack.

Eavesdropping attack, in a cloud environment which results in information disclosure can be minimized by enforcing proper authorization procedures and by transmitting the data over a secure connection such as HTTPS. Encrypting the transmitted data and attaching a signature to the same can help the destination to ensure the integrity and authenticity of data. Adopting privacy-enhancing protocols which minimize the requirement of transmitting identity credentials from the cloud service user to the verifier will discourage the illegal activity of eavesdroppers. Authentication Protocols that protect

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

secrets, ensures user anonymity and Password Authenticated Key exchange (PAKE) protocols are much preferred in a multi-tenant cloud environment.

4.2 Man-in-the-Middle Attack (MITM): Since the inception of Web 2.0, MITM has become quite popular in the SaaS environment. Here the attacker intercepts the communication channel established between legitimate users and modifies the communication between client and server without their knowledge [15].The following paragraphs discuss the various types of MITM attacks.

i) Wrapping Attack: A XML Signature wrapping attack applicable to web services is applicable to cloud as well, since cloud consumers use web services as a tool to access cloud services. This attack is launched by duplicating the credentials in the login phase by modifying the Simple Object Access Protocol (SOAP) messages exchanged between the browser and the server during communication set up [16]. The attacker modifies the signed request of a legitimate client by moving the original message body to a newly inserted wrapping element inside the SOAP header. A new body containing the unauthorized operation the attacker wants to perform with the original sender's authorization is inserted in the position of original message. The service executes the modified request since it contains the signature of a legitimate user. As a result, the adversary is able to intrude in the cloud and can run a malicious code to interrupt the usual functioning of the cloud servers. Fig 2 illustrates an application of wrapping attack. Here, the authorized client requests a picture called "me.jpg". The attacker intercepts and modifies the SOAP message by inserting the same elements in the request of the authorized client, but the name of the picture is modified to "cv.doc" instead of "me.jpg" as shown in fig 3. The server on seeing the signature of the authorized client processes the request and sends back the "cv.doc" back to the client.

The possible countermeasure would be using a combination of WS-Security with XML Signature to sign particular element and using digital certificates such as X.509 issued by trusted certificate authority (CA's). Kazi et al. [17] suggest increasing the security during the message passing from the web server to a web browser by attaching a redundant bit (STAMP bit) with the SOAP header which will be toggled when message is intercepted.

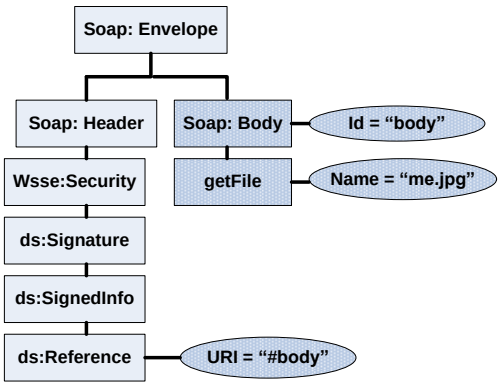

Fig 2. SOAP Message with Signed SOAP BODY – Before Wrapping Attack [7]

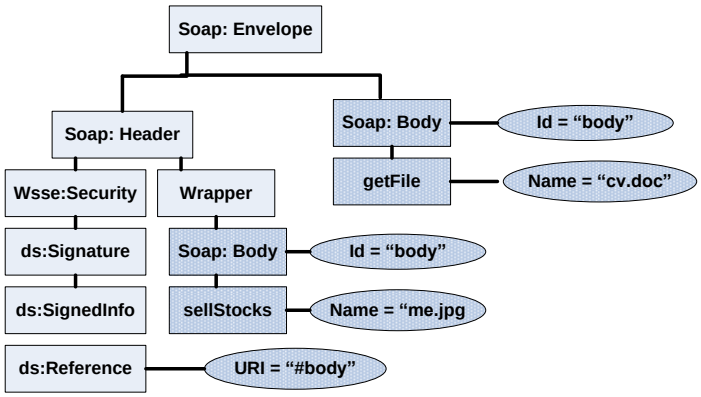

Fig 3. SOAP Message with Signed SOAP BODY – After Wrapping Attack [7]

Since the attack involves tampering with contents of the original message, attaching the hash values or the Message authentication code of the message along with the transmitted message can help to check the integrity of the message.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

ii) Flooding Attack: In a cloud environment, all the computation servers work in a service specific manner, with internal communication among themselves [16]. A successfully authorize adversary can easily send bogus request to the cloud. The cloud server before providing the requested service, checks for the authenticity of the requested jobs and the process consumes CPU utilization, memory etc. Processing of these bogus requests, make legitimate service requests to starve, and as a result the server will offload its jobs to another server, which will also eventually arrive at the same situation. The adversary is thus successful in engaging the whole cloud system, by attacking one server and propagating the attack further by flooding the entire system.

Flooding attack can be handled by organizing all the servers providing a specific cloud service as a fleet and these servers communicating among themselves regarding the incoming requests by message passing [17]. Again a hypervisor can be used to schedule the requests among the fleets, determine the authenticity of the requests and prevent the fleets from being overloaded with bogus requests from an adversary. This attack can be controlled by data transfer throttling, fool proof authentication mechanisms and mechanisms that filter out bogus requests.

iii) Browser Attack: This attack which results in data stealing is committed by sabotaging the signature and encryption during the translation of SOAP messages in between the web browser and web server, causing the browser to consider the adversary as a legitimate user and process all requests, communicating with web server [16]. For authenticating the clients, current web browsers rely upon SSL/TLS as they are not able to apply WS-Security. Nevertheless, SSL/TLS only supports point-to-point communications and this makes the authentication process insecure. Also SSL/TLS has been broken by MarlinSpike [7] using "Null-Prefix Attack" and attackers are able to perform this technique in order to request services from cloud systems without a valid authentication [18].

The potential counter measure for this is that the vendors that create web browsers apply WS-Security concept, which works at message level, within their 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.

iv) Impersonating Attack: Here the adversary pretends to be a valid server or user and lures a valid entity to reveal the authenticating credentials which in turn is used to gain unauthorized access to the resources. Verifier Impersonation attack, Phishing attack etc. can be categorized as impersonation attacks. Most of the times, in Phishing attacks 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. In verifier impersonation attack, the attacker pretends to be the verifier and lure the customer to share the authentication keys or data, which may then be used to authenticate falsely to the verifier. . In November 2007, an employee of SaaS vendor, SalesForce was victimized by a phishing attack which resulted in the exposure of the SalesForce account information of some customers [19].

In a cloud environment this can be mitigated by using two-factor and multi factor authentication mechanisms that rely on personally identifiable information (PII) in addition to passwords. Also privacy enhancing protocols that protect secrets and avoid storage of secrets can help to keep impersonation attacks under control.

v) SSL Attacks: Secure Socket Layer (SSL) is a fundamental security mechanism that encrypts the information transmitted between client and server. SSL provides an authenticated environment for running a cloud service by verifying the identity of the communication parties [20].

a) Stripping Attack: There are no standards for the issuance of conventional SSL certificates and hence client applications called relying parties cannot have confidence that the organization listed as the owner of the certificate is in fact the owner. This weakness of SSL is exploited in the stripping attack [21] which is launched by embedding a null character ('\0') in a domain name containing the name of a valid certifying authority. When SSL client software reads the domain name of the fake certificate, it will stop at the null value which is treated as a string terminator. Since the null value appears immediately after the name of a valid certifying authority, SSL client treats the certificate as a valid one.SSL Strip attack could be used

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

against Server-Server communications with the potential for mass compromise of confidential data. This spoofing problem is solved by proper use of Extended Validation (EV) SSL certificates for authentication as they contain only authenticated organization information.

b) SSL Sniffing: SSL is built on asymmetric key cryptography, involving the use of a private and public key. The public key is dispatched to the client by the server in the form of certificate signed by the certifying Authority (CA). The intermediate CA certificates, does not guarantee the legitimacy of the website and are not embedded in the browser. This limitation of SSL certificate can be misused by the attackers to launch an SSL Sniffing attack.

The potential counter measure for SSL attacks is for vendors to create web browsers that apply WS-Security concept. Instead of the point-to-point encryption provided by SSL/TLS, WS-Security provides end-to-end encryption and does not have to be decrypted at intermediary hosts. Consequently, attackers are unable to sniff and gain plain text of SOAP messages at the intermediary hosts.

4.3 Cookie Poisoning: In cookie poisoning, the identity related credentials stored in the cookies of an authorized user are modified by the attacker to gain unauthorized access to resources. Cookie poisoning attacks in cloud can be mitigated to a certain extent by using Intrusion prevention products that examines each HTTP request sent to the web server [22]**.** This attack which involves tampering with data can be handled by attaching the hash values of the data stored in the cookies and recalculating the same at the destination. Use of Message authentication codes, tamper resistant protocols and Digital signatures can also aid in the detection and prevention of modifying the cookies.

4.4 Replay Attack: In a capture-replay attack the authentication message contains the same authentication tokens previously exchanged between an authorized user and sender and was sniffed by the attacker [23]. The key to handle replay attack, which involves identity spoofing, is to ensure that something in the message changes each time. Considering this aspect, many protocols use time stamps or randomly generated nonce values to resist replay attack, which enables the verifier to check the freshness or the authenticity of the message. The usage of time stamps demands synchronization of timing at both the cloud service user and verifier end, which may not be feasible in a distributed cloud environment. Hence randomly generated nonce values are more preferable in a Cloud environment and since these values are unique for each session the receiver will be able to identify a replay of the previously send message containing an old nonce value.

4.5 Session Hijacking: Session hijacking is possible, if the Session ID issued to the authenticated users is not protected properly, which in turn can be used for spoofing identity. Session side-jacking uses packet sniffing tools to capture a login sequence and thus gain access to the user's session key Encrypting the communication channel can prevent this type of Session hijacking attack.

These attacks exploiting the loopholes such as insecure communication protocols and unencrypted data can be thwarted by using a secure communication protocol such as HTTPS, by encrypting the files that store user or administrative login credentials etc. A strong authentication mechanism that rules out the possibility of unauthorized authentication and mechanisms that protect secrets such as session keys or avoid the storage of secrets is required in a cloud environment to prevent such attacks. The side-jacking attack can be mitigated by avoiding the transfer of session keys across the communication channel. A key exchange mechanism, that involves the calculation of session key separately by the client and server, resulting in the same key value, can also be adopted.

4.6 Shoulder Surfing Attack: The attacker gains knowledge of the secret credentials such of the victim by covertly observing his entry of sensitive data via the keyboard. In public places, this attack is launched by using spy cameras. Even a partially successful shoulder surfing attack can be dangerous when used with other security threat combinations. For instance the password length information obtained by shoulder surfing attack can be used to launch a password discovery attack. This attack results in information disclosure and in a cloud scenario it can be mitigated by using secure two factor authentication and out-of band authentication mechanisms.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

4.7. Cloud Malware Injection Attack: The attack aims at injecting a malicious service implementation or virtual machine instance, which appears as one of the valid service instances running in the cloud. The adversary launches the attack by creating its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS) and injects it into the cloud. If the attacker is successful, then the cloud system treats the new instance as a valid instance for the particular service attacked by the adversary. The server thereafter starts redirecting the valid user requests to the malicious server implementation and the adversary's code is executed. The code can carry out different activities such as eavesdropping via subtle data modifications to full functionality changes.

One way of tackling this attack is to store a hash value on the original service instance's image file and comparing with that of all new service instance images. If a modification is done to a valid service instance, then the hash value will be modified which indicates the presence of an attacker. Again if a new service instance is created by an attacker and inserted into the cloud, then it should have a hash value similar to that of an existing one. But the probability of creating a service instance with a hash value, similar to the hash of another service instance is almost negligible.

4.8 Password Discovery Attacks: Attackers adopt several mechanisms to retrieve passwords stored or transmitted by a computer system to launch this attack. A few strategies adopted depending upon the availability of information related to the password are discussed in the following paragraphs:

i) Guessing Attack: Most often people use easy to remember passwords which make them vulnerable to guessing attack. An adversary observes some information related to the password, tries to guess it and then verifies it by trying to login multiple times until he gets the access. In offline scenario, the attacker has a high chance of guessing the right password as there is no restriction on the number of attempts he makes. But in online guessing scenario the system blocks the user after a certain number of login attempts.

ii) Brute Force Attack: This attack is launched by guessing passwords containing 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 demands a lot of computing power and time to be successful.

iii) Dictionary Attack: Here the attacker tries to guess a password from a pre-computed dictionary of passwords. To resist this type of an attack, the password should be random and should not be a dictionary word. Even passwords in mother tongues are not secure as attackers have dictionaries of most of the regional languages [15].

iv) Video Recording Attack: In such type of attack launched in public places, the attackers with the help of camera equipped mobile phones or miniature camera captures the password while the victim enters the same.

v) Stolen Verifier Attack: The attacker performs this attack by accessing the password table stored at the verifier. Then he launches an offline guessing attack by running a script which performs hash on each entry of the dictionary and compares the generated message digest with the stored digest of the verifier, until a match is found. This attack can have a disastrous effect in a cloud environment hosting data belonging to multiple customers.

The above discussed password discovery attacks, focuses on obtaining the password of a legal user which in turn is used to illegally impersonate the user to a verifier. Such attacks will result in a successful authentication, if and only if the authentication process is solely based on static passwords. In a cloud scenario, this can be mitigated by using graphical passwords, one-time passwords, avoiding the storage of passwords, using Zero Knowledge Proof (ZKP) mechanisms, protocols implementing 2-factor authentication mechanisms without password tables etc.

4.9 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 normally done by creating parallel session is launched by an unauthorized user to establish a valid session with the server. The attacker impersonates a valid user and requests a login session to the server. The server, as part of authenticating the requester, sends him a challenge and requests the attacker to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

send back his secret response. Since he is not a legitimate user, the attacker will not know this secret. He creates another session and sends to the server, the secret received from the server in the first session. In response, when the server replies with another secret, the attacker uses this in the first session which will be validated by the server. The attacker thus gains access to the system resources with the privileges of a legal user. In March 2013, the antispam provider, Spamhaus was hit by a special type of reflection attack leading to one of the biggest denial of service attacks ever seen, producing over 300 gigabit in traffic[24].

In a cloud scenario, keeping track of the sessions and the secrets used for each session as well as limiting the number of established sessions can help to minimize reflection attacks. 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.

4.10 Customer Fraud Attack: This is a special type of attack where in the client deliberately compromises its authentication token. The attack can be done to take personal advantages or to defame the organization. To prevent this type of attack, the verifier must be able to prove that the authentication failure was the victim's own fault [25]. In a cloud scenario this attack can be 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. This secret needs to be submitted to the verifier by the customer to pass the authentication process.

4.11 Denial-of-Service (DOS Attacks): The main objective of DOS 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. Cloud system is more vulnerable to DOS attacks, since it supports resource pooling. This attack on availability 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 and by limiting the allocation of network bandwidth. An authentication protocol that does one level of authentication at the client side will reduce the overhead of authentication process at the server side.

4.12 Insider Attacks: 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 misused his right to access the sensitive resources of the organization that negatively affected the confidentiality, integrity or availability of the organization or organizations information systems [26]. In a cloud environment an insider can be a rogue cloud provider administrator, the employees in the victim organization that exploits cloud weaknesses for unauthorized access, and the insider who uses cloud resources to carry out attacks against the company's local IT infrastructure [12]. The Cloud provider must have demonstrable security access control policies and technical solutions in place that prevent privilege escalation by standard users, enable auditing of user actions, and support the segregation of duties, and principle of least privilege for privileged users in order to prevent and detect malicious insider activity.

V. CONCLUSION

Cloud computing is a fast growing technology that offers a wide range of benefits to small and medium enterprises. But security, privacy and trust are the major concerns preventing the mass adoption of cloud. A cloud environment that provides varied services and hosts multiple resources can be secured only by allowing legitimate users to access the resources. Hence strong user authentication mechanisms restricting illegal access are the primary requirement for securing cloud. A user authentication mechanism designed for cloud should be strong enough to protect cloud from various possible authentication attacks. This work surveys the authentication attacks on cloud and the corresponding mitigation measures..

REFERENCES

[1] S. Subashini and V.Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, vol. 34, ,no.1, pp. 1 -11, 2011

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

[2] H. Lv and Y. Hu, "Analysis and Research about Cloud computing security protect policy", *in Proc. IEEE Int. Conference on Intelligence Science and Information Engineering*. pp. 214-216, 2011
[3] A. Bakshi and B.Yogesh, "Securing Cloud from DDOS Attacks using Intrusion Detection System in VM*," in Proc. IEEE Second Int. Conference on Communication Software and Networks*., pp. 260-264, 2010
[4] N.S Chauhan and A.Saxena, "Energy Analysis of Security for Cloud Application," in Proc. Annual IEEE India Conference, pp. 1-6, 2011
[5] 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
[6] X. Yu and Q. Wen, "A view about Cloud data security from data life cycle,(2010)," in Proc. IEEE Intl. Conference on Computational Intelligence and Software Engineering, pp. 1-4, 2010
[7] M. Jensen, J.Schwenk, N. Gruscka and L.L Iacono, " On Technical Security Issues in Cloud Computing," *in Proc. IEEE International Conference on Cloud Computing*, pp.109-116, 2009
[8] 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
[9] T. Hsin-Yi, M.Siebenhaar. A.Miede, H.Yulun, and R.Steinmetz, "Threat as a Service? The Impact of Virtualization on Cloud Security," *IT Professional*, vol. 14, Issue:1, pp.32-37, 2011
[10] B. Sumitra and M. Misbahuddin, "A Survey of Traditional and Cloud Specific Security Issues", Security in Computing and Communications, Communications in Computation and Information Science, Springer Verlag, Vol.377, pp 110-129, 2013
[11] Rohit Bhadauria and Sugata Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques," *International Journal of Computer Applications*, pp. 47-66, 2012
[12] William R ClayComb, Alex Nicoll, "Insider Threats to Cloud Computing: Directions for New Research Challenges", [Online], www.cert.org/archive/pdf/CERT_cloud_insiders.pdf
[13**]** Larry Hardesty, "Thwarting the Cleverest attack", May 1, [online] web.mit.edu/newsoffice/2012,thwarting-eavesdropping-data-0501.html,2012
[14] Maventek, Cloud *Security Consulting* [WWW] Available from: www.maventek.com/services/Cloud-security-consulting, 2012
[15] M.Misbahuddin, "Secure Image Based Multi-Factor Authentication (SIMFA): A Novel approach for Web Based Services, Ph.D Thesis, Jawaharlal Nehru Technological University, [Online], http://shodhganga.inflibnet.ac.in/handle/10603/3473, 2010
[16] B.Meena and K.A. Challa , "Cloud Computing Security Issues with possible solutions," *Int, Journal of Computerr Science and Technology*, vol.2, Issue: 1, Jan–March, 2012
[17]Kazi Zunnurhain and Susan V. Vrbsky,,"Security Attacks and Solutions in Clouds, [Online] http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf, 2010
[18] Danish Jamil & Hassan zaki, " Security Measures in Cloud computing and Counter measures", International Journal of Engineering Science and Technology(IJEST), Vol.3 No.4 , 2011
[19]Y.Andree, "Implications of Salesforce Phishing Incident", [Online] http://www.ebizq.net/blogs/security_insider/2007/11/implications_of_salesforce_phi.php, 2007
[20] Abel Wike, "SSL Encryption – A Protocol that Authenticate Cloud Computing", [Online] comluv.com/ssl-encryption-a-protocol-that-authenticate-Cloud-computing, Feb 5, 2013.
[21]Larry Seltzer, [Online] Spoofing Server-Server communication: How can you prevent it" https://otalliance.org/resources/EV/SSLStrip_Whitepaper.pdf, 2009
[22] Imperva (2013), *Cookie Poisoning* [WWW], Available from: http://www.imperva.com/resources/glossary/cookie_ poisoning.html 2013
[23] Mark O' Neill, Blog: Connecting SOA to the Cloud, Friday, September 4, 2009, Replay Attacks: Why "If it works twice, then it doesn't work" makes sense , [Online] http://www.soatothecloud.com/2009/09/replay-attacks-why-if-it-works-twice-it.html,2009
[24] Lucas Kauffman, "About the recent DNS Amplification attack against Spamhaus: Countermeasures and mitigation", [Online], Security.blogoverflow.com/2013/04/about-the-recent-dns-amplification-atatck-against-spamhaus-countermeasures-and-mitigation,2013
[25] Umair Ashraf, "Securing Cloud Using Two-Factor Authentication – M.Sc Infotech- thesis", ftp://ftp.informatik.uni-stuttgart.de/pub/library/medoc.ustuttgart_fi/MSTR-3452/MSTR-3452.pdf,University of Stuttgart, 2013.
[26] 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) ser. SEI series in Software Engineering. Addison-Wesley Professional, 2012.