International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Data Security in Cloud Security Attacks and Preventive Measures

Monica Gadre[1], Shruti Chincholkar[2]
[1, 2] *M. Tech Scholar: Dept. of Computer Science and Engineering Vellore Institute of Technology, Vellore, India*

Abstract: Authentication, Availability, Integrity, Confidentiality and nonrepudiation are the five pillars of Data Security. Data Confidentiality, Authentication and Integrity are breached when a user's data is stolen by the intruder. Confidentiality of data is obtained by keeping the data safe and intact, which means that the sensitive information of the user should not be disclosed to anyone. Authentication is the process through which the user is authenticated; this can be done by implementing passwords/PIN on the user's data. If the user is a legitimate user he/she is allowed to access the data. Data Integrity ensures that the data is recorded as it is intended to be and upon the retrieval of data at any time in future the originality of the data should be maintained. Cloud stores huge amount of data that are stored at a single place. Data is stored and accessed by various devices and resources which are shared by many different users which increases the risk of attacks. Cloud Data can be stolen by different attacks few of these attacks are mentioned in the paper. The stolen information is used by the attacker to perform malicious and unauthorized activities. This paper focuses on the attacks and the prevention measures that an end user can follow to keep this data safe from being disclosed attacked by the attacker.
Keywords: Cloud Computing; Cloud Service models; Deployment Models; Data security; Cloud Attacks

I. INTRODUCTION

Cloud computing is an information technology (IT) paradigm, which allows users/companies to utilize various computing services. These computing resources can be anything like memory, speed, software etc. Companies providing these services are called cloud providers and they charge according to the usage of that particular service. Cloud Computing has attracted many companies like Amazon, IBM, Google etc.

A. Service Models

There are three basic cloud service models-They are PaaS, IaaS, and SaaS. Platform as a Service (PaaS) vendors provide end user a platform to develop and deploy applications/software. In this Model, the cloud providers provide a platform to compute, that includes operating system, databases, and web servers. The users can develop and deploy there application and test it on the Platform provided by the cloud provider. Few PaaS Providers include Heroku, Google App Engine, SAP and Intuit. Infrastructure as a Service (IaaS) vendors provide their resources with dashboards and API's. It is the most flexible cloud computing model. IaaS also offers additional resources like firewalls, load balancer, file or object storage, IP Addresses etc. Examples of IaaS providers are Navisite, Exoscale, Citrix and Softlayer In Software as a Service (SaaS) model, users get access to the databases and application software. It is also known as "on-demand software"(user gets access to the requested software when needed) and is priced on a pay-per-use basis and is not charged anything additional. Examples of SaaS applications are Salesforce, Google App, LiveOps, Taleo and Joyent.

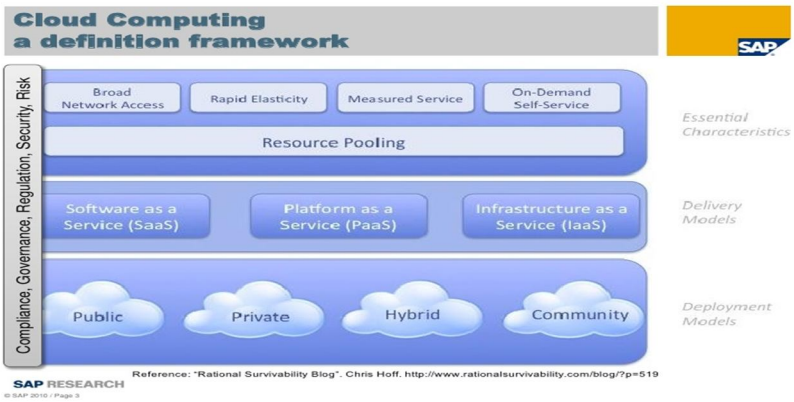


Figure.1-Cloud Computing Framework

B. Cloud Deployment Models

Cloud deployment model are of three types-Public, Private and Hybrid. They are distinguished based on the ownership, size and access

1) *Public Cloud:* It is a cloud infrastructure which is publicly accessible by everyone. The cloud provider is responsible for the maintenance of public cloud. Public cloud is less secure as it can be accessed by anyone. Few public cloud providers are Amazon AWS, Microsoft Azure.
2) Private Cloud: It is a cloud owned by a particular organization, managed internally or by a third-party. Implementation of private clouds can be expensive and cannot be adopted by small or medium sized organizations. Private clouds are driven by concerns regarding security and complianc
3) Hybrid Cloud: It is complex cloud environment of two or more cloud models combined together depending on the user's needs. Hybrid cloud architecture can be complex and difficult to create and maintain.

This Paper will focus on the data security issues in Cloud. The Section II is the review of the literature that provides the contribution already done in this area. Section III gives a detailed description about the types of threats to data in the cloud environment. The Section IV gives us the common approach to perform the attacks. Section V focuses on the encryption of cloud data. Section VI provides with the preventive measures that can be taken to secure the data stored or accessed through cloud. The final section concludes the study.

II. LITERATURE REVIEW

In order to understand the basics of cloud computing and storing data securely on the cloud, several resources have been consulted. This section provides a review of literature to set a foundation of discussing various data security aspects.

Ahmed Albugmi, Madini O. Alassafi and Robert Walters, Gary Wills provided an excellent insight into the basic concepts of cloud computing. Several key concepts of data security are explored in this paper. It provides detail of data protection methods and approaches to ensure maximum data protection by reducing risks and threats.

Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy defined cloud computing, the various cloud models and security risks and issues that are currently present within the cloud computing industry. The paper also represents various challenges in cloud computing and offers best practices to service provider.

Most common attack in cloud is account hijacking thus A. Annie Christina provides information on account hijacking and various proactive measures on hijacking. It also discusses basic proactive measures that can be taken to prevent or in other words minimize to the stealing of the user account details and services.

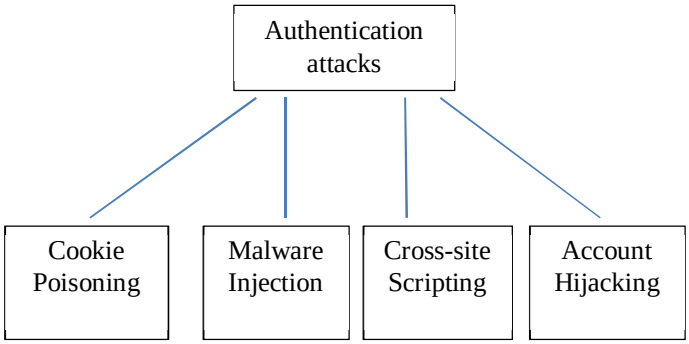
B. Sumitra, C.R. Pethuru, M.Misbahuddin described the various authentication attacks that can be performed over the cloud data.

Sreenivas Sremath Tirumala, Hira Sathu and Vijay Naidu described regarding the account hijacking attack over the cloud environment. They have focused on the phishing attack to hack/hijack the account.

III. THREATS TO DATA IN CLOUD

Data Security depends on the three service models: PaaS, SaaS, and IaaS. Two sets of data have threats to its security: They are- Data at Rest and Data in Transit. Data at Rest refers to the data in cloud (live data) or the data stored in cloud. Data in transit is the data that keeps moving in and out of cloud. Data in transit is more vulnerable than data at rest, as it keeps moving from one location to another over the network.

Few common attacks in cloud are mentioned below-



A. Cookie Poisoning

Internet Cookie is a small set of data from a website stored on the user's system by the web browser while he/she surfs the internet. They are used to record the user's browsing activity and to store arbitrary information which the user has previously entered into form fields.

Authentication cookie are the most common method used by the web server to know if the user is logged in/off the session and which account is he/she logged in. Without such mechanisms the site would not know whether to send a page containing sensitive information. Security vulnerabilities allow the cookie information to be read by a hacker which can be used to gain access to the user's data.

Advantages of using cookies-

1) User identification and authentication
2) Statistics on number of visits
3) Storing preferences and settings

In Cookie Poisoning, an authorized user's identity related information which is stored in the cookie is modified by the intruder to gain unauthorized access to the user's resources. The attacker can use the stolen information to create new accounts or gain access over the user's existing account.

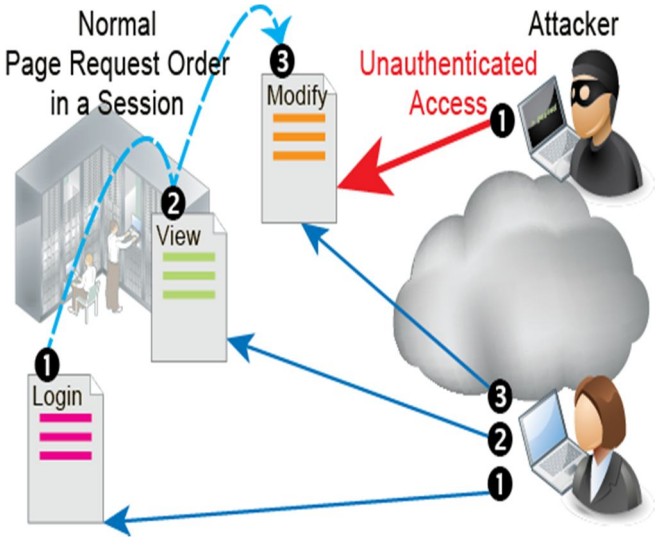


Figure-2.Cookie poisoning attack

B. SQL Injection

Structured Query Language is known as SQL is used to interact with the database. SQL queries like create, insert, delete and update are used to perform actions on the database.

SQL injection is a malicious SQL command injected in cloud services source code that helps attacker gain access and allows intruder to perform unauthorized task over the data.

When the injection is executed and the cloud begins to operate, attackers compromise the confidentiality and integrity of sensitive information and can steal data. SQL injection (SQLi) is a security weakness of the website that allows attackers to access the database of the application by letting the access or change of data.

Using this method unauthorized access is gained by the attacker over the database and security of database is breached.

By using SQL commands user can accomplish the following attacks –

1) Bypassing the Login of the user
2) Accessing the confidential data
3) To access and modify the content

The main idea behind the SQL Injection attack is that an attacker transfers a manipulated SQL code so that attacker can gain access to the website database.

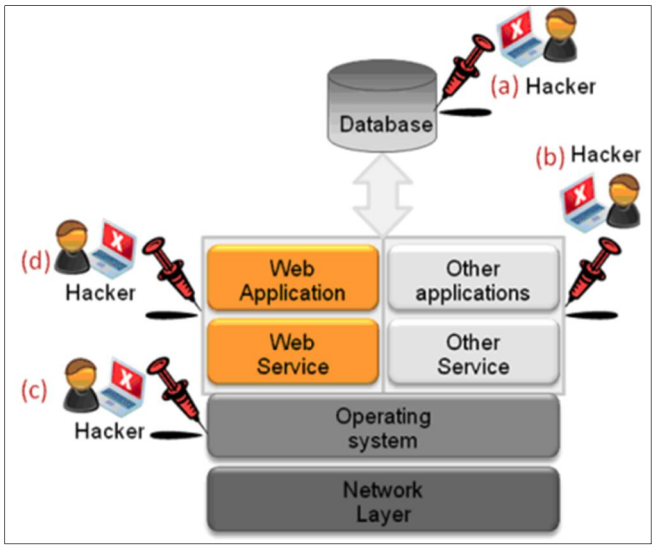


Figure.3.SQL injection

C. Cross-site Scripting

In this attack, the user is redirected to an unsecure website and the attacker gains access to the user's credentials. The user enters the correct URL and is redirected to the attacker's website.

Cross Site Scripting is a security attack performed on dynamic web pages where an attacker can create a malicious web page of the original cloud site to inject unwanted executable code into a Website.

Cross-Site Scripting occurs when

1) When a web request is made by the user data enters a Web application through an untrusted source.

2) The data is added to the dynamic content which is sent to the user without validation.

This attack can be implemented by creating a fake webpage which is similar to the cloud provider website. The user thus gets an illusion and inputs the login credentials to that webpage. These credentials are sent to the attacker. The attacker can thus gain access over the users account and perform malicious activity.

For example - The domain in this case is www.mycloud.com. The actual URL is varied by inserting some other text into it (i.e. add a "y" after my). This will trick the user as he assumes it to be the real cloud site. The user will login in into that URL and thus the attacker will get the login details.

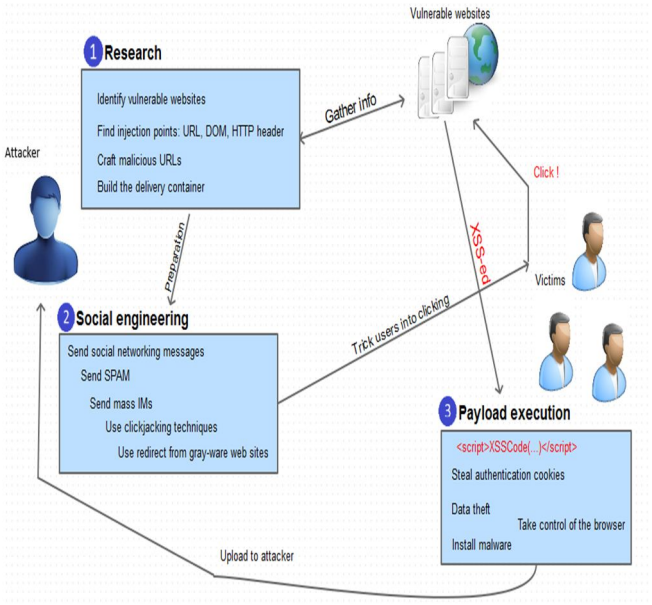


Figure-4. Cross-site Scripting

D. Account Hijacking

In account hijacking attack the attacker can use the login credentials to remotely access sensitive data stored in cloud and he even has access to modify and falsify information through hijacked account.

Cloud account hijacking is an attack in which the cloud account credentials are stolen by the attacker. When account hijacking occurs over cloud, an attacker uses an email account or other credentials to breach the account owner's data.

1) *Ways of account hijacking:* Account hijacking can be done via phishing i.e. sending spoofed email to the user or by applying brute force attack i.e. guessing the password or by using some other hacking methods. The account hijacking uses different methods to obtain the personal data of cloud user. These two are most commonly used –
2) *Hijacking by Phishing* – The phishing attack involves a recipient e-mail that appears to be from a legitimate cloud provider. The e-mail has content that informs the user that there is some problem with the users account like password expired and user clicks on the link given in the email to solve it. But in reality, the fake email and the hyperlink is simply collecting customer user names and passwords for attacking over accounts.
3) *Hijacking by Spyware* - Spyware is loaded in the cloud account or system when the user opens a spoofed e-mail attachment or clicks on a popup advertisement. It then collects the personal information (i.e. Username, password and account numbers) and forwards it to the attacker.

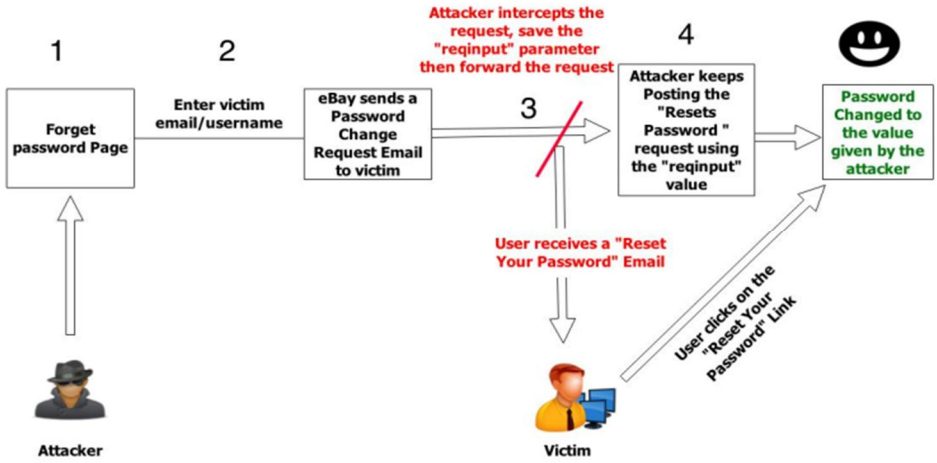


Figure-5.Account Hijacking attack.

IV. PROPOSED METHOD

There are many different ways to perform the attacks mentioned above. We describe one of the approaches in this section and the tools used to perform the attack.

A. Cookie Poisoning Approach

Cookie Poisoning is similar to parameter tampering. It stores the Sensitive data of the user like the username, passwords, rights are privileges etc.

B. Tools used- Parasproxy

The user can perform the normal operations on a website (login, select items, make payments etc.). We need to go to the parasProxy tool, go to the trap option and check the trap-request and trap-response options. Go back to the browser; we need to make changes in the browser settings.

Go to the internet settings options in tools, then click the connection tab and go to LAN Settings,

In the LAN Settings window, check the option use a proxy server and set the address and the port to-

Address- localhost

Port- 8080(Default port) and then click OK.

Try performing a operation on the website and go to the parasproxy tool.

The parasproxy tool will have the details of the cookie trapped in it. It provides us with the cookie details like the session id, the privileges a user has and other information regarding the user.

We can make changes to the user's data and get access to his account and the user privileges.

B. Sql injection

The following steps need to be followed for SQL injection over cloud –

1) The user enters the login credential.
2) One way is by providing the wrong input. Suppose user tries to enter some other commands along with the actual login details (like drop table table_name ;)
3) In this way the malicious user injected the code that deletes the whole table.
4) Other way can be by trying to inject the wrong user credentials by varying the login page source code of the cloud providers site i.e. by writing some command that always provides a true value so that attacker gets logged in.
5) This is done by changing the username and password by using the command select *from users where username='1' or '2' = '2' and password='1' or '2' = '2 ';
6) By this we get an access to the cloud website.

C. Cross-Site Scripting Approach

In this approach, we redirect the user to a cloned
Website (attacker's website).It is an attack to steal the user credentials.
TOOLS USED- Kali Linux, Set Toolkit
Set Toolkit is a tool used to perform various social engineering attacks. It gives a menu to choose the attack that the user wants to perform. The user needs to select the options, in this case we select the website attack vector.
Under website attack vector we choose to clone site. We need to provide the IP Address of the system and the URL of the website that you want to clone. As we need the user credentials we would provide the login URL. For redirecting the user we need to change the code in the login page. The user would be redirected.
(Using Burpsuit, DVWA we can redirect the user). Go back to SetToolkit to check the location were the credentials get stored.
Trace the location to find the user's login credentials.
We get the user's details and the data can then be manipulated /stolen.

D. Account Hijacking Approach

The approach for account hijacking using phishing method is given -

1) Create an html page of website with the source code similar to actual cloud provider's website.
2) Name the file by similar name of the website i.e. if the website name is https://www.revion.com then change it to https://www.reviion.com so as to provide the illusion that it is a real site.
3) Now create a PHP script that sends the username and password to the attacker. The credentials will be sent to the email acco
4) For performing this, change the action part of the login.html page in copied code .i.e. http://www.revion.com/login.html id=attackerid@gmail.com & link=fakelink.com
5) Now send this fake webpage as a link to the user so that he feels that the mail is from the actual cloud provider and clicks on the link. When the user provides the credentials and logs in, he will be redirected to the actual website and the attacker will get a mail containing the credentials of the user.

V. ENCRYPTION IN CLOUD

Due to the threats and challenges in cloud, it is necessary to encrypt the customer's/end users data in cloud, which requires encryption mechanisms. In cloud encryption mechanism the end users data is converted to a cipher text.
In the process of encryption the user's data passes through mathematical formulae know as Algorithms. The data can be encrypted using different algorithms depending on the sensitivity of the data. Few Algorithms that can be used on cloud data are RSA, Diffie Hellman, AES, DES, XTR, Digital Signature Algorithm etc.

A. The Two Types Of Encryption Are

1) Symmetric Encryption
2) Asymmetric Encryption

B. Asymmetric Encryption

In the asymmetric encryption process there are two mathematically related keys used- the public and private key. One of the keys is used to encrypt the data and the other pair of key is used to decrypt the data.

Major part of public key are-
Plain text, Encryption Algorithm, Pair of private and public key, Cipher Text and the decryption algorithm.

C. Steps of Asymmetric Data Encryption Process

1) The text gets converted to a pre-hash code using the mathematical generated code formulae
2) The pre hash code is encrypted by the software using the sender's private key. Using the algorithm used by the software private key would be generated.
3) The encrypted message and the pre-hash code are again encrypted using the sender's private key.
4) To retrieve the public key of the person this information is intended for sender of the message.
5) The secret key is encrypted by the sender using the recipient's public key, therefore only the receiver can decrypt it using the private key, thus concluding the encryption process

Asymmetric encryption provides more security to the cloud data but it is computationally slower than the symmetric key encryption.

D. Symmetric key Encryption

In this process on encryption there is only a single key (secret key) used both by the sender and the receiver. The sender uses the secret key to encrypt the data and the receiver uses the secret key to decrypt the data. The secret key should be known to both the parties to encrypt and decrypt the data.

VI. PREVENTION FROM CLOUD ATTACK

A. These Are Some Measures That Can Be Taken To Protect Data

1) *Password Protection :* If the password is easy to remember for user, it can also be easy for the hacker to figure it out. The password must have combination of letters and numbers. It must not have names of things related to user, or contact number and similar data that is easy to be cracked by the attacker.

2) *Anti-Spyware:* Anti-spyware software is a program designed to detect and prevent spywares and thus it must be installed by every computer connected to the internet

3) Antivirus software: Anti-virus software is a program aimed to detect, prevent, and remove the viruses and other malicious software (e.g. worms, Trojans, adware, and more) from the internet.

Phishing Awareness – If user receives an unexpected email, or one that you consider suspicious, then clicking on the attachments or opening the mail must be avoided

VII. CONCLUSION

Cloud computing allows to store and process the data. It relies on sharing of resources, so the cloud security is a major concern. Along with that, increase in user data there is a need for a bigger storage space. Cloud provides a solution to store large amount of user data. As huge amount of data is available on cloud there is a need to secure the data and to keep it safe from being attacked or stolen. This paper discussed about the security of data over cloud. The attacks possible over cloud are explained. For the better explanation the visualization of some attacks like account hijacking using phishing, SQL injection, cookie poisoning and cross-site scripting is done. This helped us gain information about the attacks possible over cloud and the way in which these attacks are performed from the attacker's perspective. The paper also provided basic solutions and some preventive measures for these attacks

REFERENCES

[1] http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt.
[2] http://www.trp.org.in/wpcontent/uploads/2015/12/AJCST-Vol.4-No.2-July-December-2015pp.31-34.pdf
[3] https://ciphercloud.com/wpcontent/uploads/2014/11/Tech-Note-Account-Hijacking-Dyre.pdf
[4] https://dome9.com/wiki/display/cloudsecurity/Account+Hijacking#AccountHijacking
[5] http://www.ijcsits.org/papers/Vol1no22011/13vol1no2.pdf
[6] A. Annie Christina, Proactive Measures on Account Hijacking in Cloud Computing Network, 2015
[7] Tejinder Singh, Detecting and Prevention Cross –Site Scripting Techniques, IOSR Journal of Engineering ,April.2012
[8] Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds,2010
[9] Parveen Kumar, Cloud Computing: Threats, Attacks and Solutions, IJETER research paper, 2016
[10] Ahmed Albugmi Madini O. Alassafi Robert Walters, Gary Wills, Data Security in Cloud Computing, FGCT, 2016
[11] Kalyani Kadam, Rahul Paikrao, Ambika Pawar, "Survey on Cloud Computing Security", IJETAE, December 2013.
[12] https://www.veracode.com/security/sql-injection

[13] Li Qian, Zhenyuan Zhu, Shuying Liu Research of SQL injection attack and prevention technology, IEEE publication, 2015
[14] Aley C. ,"SQL injection SQL sersver application.[EB]",http://www.creangel.com/papers/advanced_sql_injection.pdf.
[15] Nilosha Pereira, Vimukthi Elvitigala, Mahesha Athukorala, Piumi Fernando, Dineth Ehelepola, Kosala Sameera, Dhishan Dhammearatchi, “Secure User Data in Cloud Computing through Prevention of Service Traffic Hijacking and Using Encryption Algorithms”,
[16] International Journal of Scientific and Research Publications-2016.
[17] B.Smitra, C.R. Pethuru, M.Misbahuddin, A Survey of Cloud Authentication Attacks andSolution Approaches , International Journal of Innovative Research in Computer and Communication Engineering-2014