Cloud Security Issues and Impact on Social Media

K. Sharadha
III Bsc Computer Science
M.O.P Vaishnav College for Women

ABSTRACT

Social networking sites enable users to interact with others and share experiences, feelings, and opinions. When we upload a video on YouTube, the video gets stored in the cloud; when we store photographs on Flickr or post them on Facebook page, the photos are said to get stored in the cloud. Thus it makes us realise that cloud computing drives many social media sites that we access every day. Visitors can become members by registering with the social networking sites and they'll be able to send messages, store photographs, upload videos and interact with others online using the internet. But using the cloud services does have some disadvantages. Thus, the paper mainly focuses on the major cloud security issues and its impact on the social media, security measures to stay safe in the cloud and its predicted future.

Keywords

Cloud Security, Social Media, Security Measures

1. INTRODUCTION

1.1 Related Work

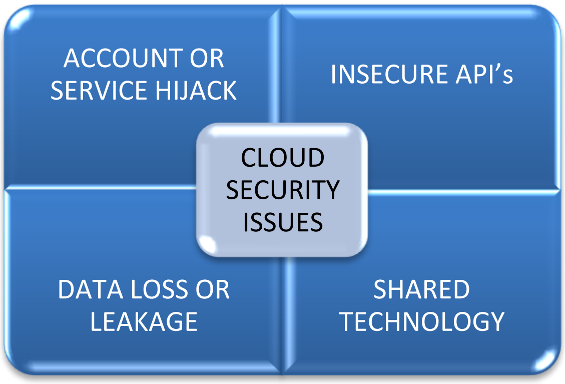
Professor Asha Mathew [1] has described about the security and privacy concerns of cloud and the possible solutions. She has also proposed a secured framework for safe cloud computing. In this frame work the clients are provided access to the network by using a secured VPN.

Nelson Gonzalez, Charles Miers, Fernando Red´ıgol, Marcos Simpl´ıci, TerezaCarvalh, Mats N¨aslund and MakanPourzandi [2] describe the analysis made on the cloud security issues and propose solutions. The paper also describes with the help of pie charts the sources of security breaches on the cloud and the various solutions. The tables summarise the ideal framework.

FarzadSabahi [3] talks about the cloud security in a different manner. The various problems such as data leakage and security breaches due to DDoS attacks against the cloud are dealt with.

1.2 Security Issues

Social media sites largely use cloud for their storage. This is because social networking sites like Facebook, twitter have to store profiles, pictures, likes and other data and cloud made storage flexible and scalable. All these advantages overshadowed few security issues and these are addressed below:



1.2.1 *Insecure APIs and Interface*

Application Program Interface (API) is a set of rules or instructions that are used for accessing a web based application. CSPs provide users/customers with a set of APIs or software interfaces to access the applications provided by them.

The availability and security of the data stored in the cloud depends largely on these API's [4]. When the APIs provided do not have architecture to prevent intentional and accidental attempts to access sensitive data, it means that issues such as data availability, integrity and confidentiality tend to arise. This is mainly because these interfaces are provided to the user as value added services and hence are not checked much by the user/customer.

1.2.2 *Shared Technology Issues*

Cloud computing is based on a business model that caters to the needs of several customers at the same time. This is also called multi-tenancy. IaaS service providers provide services by sharing infrastructure. So, attackers who try to gain access over other cloud customers' resources exploit this shared infrastructure.

An attacker should have valid login details to log in into a guest virtual machine to exploit this vulnerability. If the infrastructure is not designed to provide strong isolation in a multi-tenant environment it leads to various problems like Denial of Service (DoS).

To provide a solution to this, a virtualization hypervisor [5] is used which mediates access between guest operating system and the physical compute resources. Still, machines cannot be fully trusted, as in IaaS (Infrastructure-as-a-service) there is no stringent design/architecture that distinguishes the users from the attackers. Thus, the guest operating systems sometimes gain inappropriate levels of control.

1.2.3 *Data loss or Leakage*

Data loss or leakage is one of the most important security issues in cloud computing that needs to be addressed. When users move to cloud two changes are bound to happen with their data. First, the data will no longer be in the customer's local machine. Second, the data is now stored in a multi-tenant environment which is accessible to everyone. Thus it leads to a question over the confidentiality of data and this problem sometimes is called data leakage.

Data leakage happens due to several reasons. But the most important is that, when data is placed in the public cloud the user/organization does not have direct control over the confidentiality of the data. Hence SaaS and PaaS users are more vulnerable to data leakage problems. Data loss happens mainly when malicious intruders get control over a sensitive data. This is made possible only when there is insufficient authentication / authorization. Moreover, the other possibility is where the data centres of the CSP crashes and no proper backup is available thus leading to lot of chaos to both the CSP and the organizations. This security breach leads to huge loss for companies that are totally dependent on their data for the activities.

1.2.4 Account or Service Hijacking

It is not new to hear the word hack or hijack. While the other security issues are mainly the responsibility of the CSP this is something that is shared by the CSP and the user. With various attack methods it is nowadays easy for attackers to gain information about the users mainly if the CSP does not provide an architecture that prevents these malpractices. Methods like phishing enable attackers to get the user information/credentials as many users reuse the same username and password for several services. Thus, when an attacker gets the user credentials he gets to access all the sensitive information in the cloud and also the various transactions and activities done by the user. Hence users have to compromise on the integrity and confidentiality of data stored on the cloud.

1.3 Impact on Social Media

1.3.1 Insecure API's and Interface:

This issue of cloud computing has a great impact on social media and users of it. Social networking sites like Facebook Twitter store the profiles of all its users on what is called as public cloud. Insecure API's or interfaces means poor authentication and hence, it is easy for attackers where they can easily create fake accounts of celebrities or they can create a duplicate account of a person and add their friends. In this way attackers usually gain control over the user's account which they can further use if for other purposes.

1.3.2 Shared Technology:

With shared technology all the data that is stored is open to all and most importantly there are certain users who share their personal information such as their email ids, address and phone numbers. All sensitive information can be mined and stored by attackers [6] and can be used for those like those mentioned below:

1. The idea might be to advertise where by commenting on posts or pictures, attackers can easily distribute their links or products. This might not benefit the attacker much.

2. The other possibility might be phishing or malware installation. For example, an attacker might create a page identical to that of Facebook and might provide the link in the posts wherein when people click on the click when an identical page appears they might think they have signed out and might log in again. In this way they might promote their malware attacks and hence users of social networking sites should be careful.

1.3.3 Data loss or Leakage:

The responsibility for this is to be held by the user of social networking sites. Mainly employees of companies and companies themselves make use of social networking sites for advertising and also recruiting people. With this it enables attackers to create similar accounts as mentioned above thereby they gain access to confidential and sensitive information. Thus it leads to information leakage. Data loss arises usually because all data in the cloud is shared among thousands and millions of users and attackers in some situations gain control over the sensitive data take a backup and delete all these sensitive information.

Thus extensive use of social networking sites increases the probability of information leakage and data loss. Moreover sometimes it might even lead to expulsion or termination of employees due to violation of social networking policies. [7]

1.3.4 Account or Service hijacking:

This mainly occurs due to programming flaws or due to the user's carelessness. In the case of programming flaws attackers exploit the minute flaws in the websites. A very good example is that of Twitter where it had to face "cross-site scripting" [8]. The tweets of the users were altered by using the attackers' account thereby making users to promote certain unwanted or sensitive information.

The other is the user's carelessness, where there are certain people who leave their accounts without signing out for a long time. In this case there are certain malwares that would detect this and the users information is make available to the attackers for further use. In another case it is where while downloading certain software there are additional malware that get installed and when the username and password are entered it traces them and stores then in a database for the attackers.

2. SECURITY MEASURES

The following are some of the security measures organisations must look into before adopting the cloud:

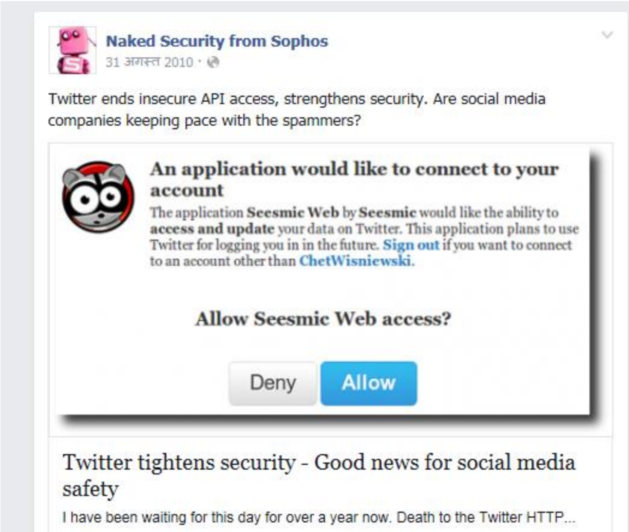
1) **Firewall:**
Proper authentication can be done by installing a proper firewall and maintaining it. The firewall must be deployed in such a way that it will be able to deny access from untrusted sites.

2) **Data encryption:**
In case of public cloud the resources are shared between the various users. Data encryption is a method that is used to safeguard the clients' data. The data is encrypted and stored or data when it is transmitted is encrypted and sent and the data is decrypted at the receivers end.

3) **SLA's:**
Users must carefully look into the security policies of the CSP and the SLA's to make sure that there are proper measures for patching and vulnerability management.

3. CONCLUSION AND PREDICTED FUTURE

Social media is thus one of largest medium of communication. It enables users to communicate, express their views and bring awareness. For this cloud computing plays a vital role. But because of the security issues like insecure APIs', shared technology to mention it has become necessary for social networking sites' administrators to protect their users from these or probably reduce these issues. Twitter has been one of them. [9]



Naked Security from Sophos
31 अगस्त 2010 ·

Twitter ends insecure API access, strengthens security. Are social media companies keeping pace with the spammers?

An application would like to connect to your account

The application **Seesmic Web** by **Seesmic** would like the ability to **access and update** your data on Twitter. This application plans to use Twitter for logging you in in the future. Sign out if you want to connect to an account other than ChetWisniewski.

Allow Seesmic Web access?

Twitter tightens security - Good news for social media safety

I have been waiting for this day for over a year now. Death to the Twitter HTTP...

The above post shows that twitter had put an end to insecure API's. In the future it is necessary for social networking sites to adopt new policies that mainly focus on data protection services and user privacy. Thus it can concluded that as social networking sites have new customers coming up every second it is necessary that the demands of its users are met and to achieve this cloud computing is the best solution and hence the future of social media heavily relies on cloud as all the data is stored in the cloud.

4. REFERENCES

[1] Security and privacy issues of cloud computing; solutions and secure framework professor: Asha Mathew assistant professor (research),welingkar institute of management development and research, Bangalore.

[2] A quantitative analysis of current security concerns and solutions for cloud computing: Nelson Gonzalez, Charles Miers, Fernando Red´ıgol, Marcos Simpl´ıci, TerezaCarvalh, Mats N¨aslund and MakanPourzandi

[3] Cloud Computing Security Threats and Responses - FarzadSabahi (Faculty of Computer Engineering) Azad University Iran

[4] Top threats to cloud computing V1.0 prepared by Cloud Security Alliance March 2010

[5] https://www.clickssl.com/blog/top-8-cloud-computing-threats-and-its-security-solutions

[6] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_security_guide_to_social_networks.pdf

[7] http://www.csoonline.com/article/2125974/social-networking-security/survey--fear-of-data-loss--security-risks-via-social-media-sites-on-the-u.html

[8] http://www.v3.co.uk/v3uk/news/2349680/twitter-scrambles-to-fix-tweetdeck-cross-site-scripting-attack

[9] https://www.facebook.com/SophosSecurity/posts/148167271872724