INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Fraud action and countermeasures in cloud

Kishore Shreyas S
shreyaskishore23@gmail.com
B. M. S. College of Engineering, Bengaluru, Karnataka

ABSTRACT

Cloud offers a very efficient computing platform that makes their customers work better in different levels of tasks. Cloud offers a variety of services such as software, application, infrastructure, and storage. In the last few years, the number of people using these services has increased more and lots of information has been stored in the cloud. At the same time, many attacks related to the cloud has also increased due to attackers trying to exploit the security vulnerabilities. Managing the cloud without any attacks is one of the important aspects and knowing the countermeasure to handle each attack is necessary to everyone who is utilizing the cloud service.

Keywords: *Cloud, Attackers, Threat, Vulnerability.*

1. INTRODUCTION

Cloud Computing has been used in our day to day activities. It gives Software as a service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Almost everyone uses the cloud on a regular basis. For mailing users connect to Gmail and Outlook; people get entertained by subscribing services such as Hotstar and Netflix; to stay connected with people and share activities about them social sites such as Facebook, LinkedIn, and Twitter are used; to store information about anything Dropbox and Google Drive are the most popular services. Google docs help in working with users on the same page. Cloud Computing has been used in almost all areas. There are many advantages of the cloud such as flexibility, scalability, reliability, mobility, sustainability, quality service, cost saving, disaster recovery. In the cloud, if the user has an access to the internet the data can be accessed anytime and from anywhere. Cloud also gives better insight.

2. NEED FOR CLOUD SECURITY

Although cloud computing has more advantages it has its own flaws related to information security and risks according to each of its service. A hacker can forcefully attack the computing efficiency working on illegal activities. Hacker mostly rents virtual machine check for vulnerabilities, see how the systems are configured and then start to give an attack to other host existing in the same cloud. IaaS gives the advantage of handling multiple virtual machines which makes hacker to perform attacks such as Distributed Denial of Service. The data is the most important part that has to be secure in a cloud. In the last few years, data theft and loss have been one of the biggest security threats to the cloud. Data in all three services can be accessed by unprivileged internal employees. Intruders simply place a virtual machine in the network to eavesdrop what information has been transferred from one host to another. When an association really thinks that they have to move their current operations to the cloud they should be known to cloud attacks and threats to make sure that the process and data of the association remain safe. Users shouldn't always depend on the service providers to safeguard the data. It is always important to find out the most possible cloud attacks and threats to make the security of the cloud effective. Security fixes and patches should also be checked and updated at regular intervals. Necessary action has to be implemented whenever some threats are identified so that it does not lead to anymore data loss or damage to the cloud.

3. LITERATURE SURVEY

Cloud computing is a group of resource that are being given on demand. Cloud service has grown significantly faster in the field of IT world due to its increased advantages. Cloud service handles data and technologies more efficiently. Cloud makes their clients to use the virtual resources over the internet as per their needs and requirements. Clients pay according to their usage of resource. It is very easy cost effective because the clients don't have to maintain or install anything. In cloud context privacy occur according to the cloud model .Cloud has three service models – IaaS, SaaS and PaaS. Apart from this there are three deployment models for

cloud – Public, Private and Hybrid. Although cloud has many advantages it has its own security threats and challenges associated with its service. Security is considered as one of the import aspects in any service. Cloud security threats and attacks are based on the nature of these cloud services. Basically cloud threats are classified into data, application, cloud service provider and network. Much vulnerability still occurs and attackers continue to exploit these security vulnerabilities. Data confidentiality, integrity and availability has to be maintained without any discrepancy in cloud and it can be only achieved where there is no data breach.

Application threats and attacks leak a lot of personal information of users helping hackers to use it in many aspects of hacking. Network attacks such as denial of service and domain hijacking also possess serious threats to the cloud. There are some similar countermeasures for all kinds of risks and threats such as access management, data protection policies, setting up a firewall, usage of IDS/ IPS, backup facilities and encryption techniques. Many new technologies have emerged which is involved in daily activities and making users lives easier. Once the organization has decided to move to the cloud technology it loses control over the data. The amount of security which is needed

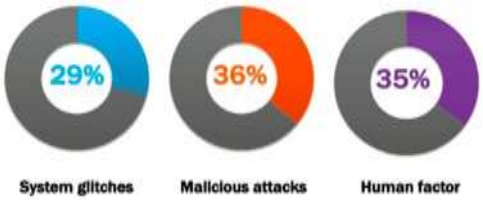

Fig 1. Main Causes of Data Breach

to protect the data is directly proportional to the value of the data. Users have to understand the risks and threats associated with cloud. For a better service and quality, security flaws must be identified and it has to be solved and made sure that it won't occur in future.

4. DATA RELATED SECURITY THREATS

Data Breach

A data attack can come from within or outside the organization. Any attacker will try to access the data stored in the cloud by doing any illegal activity. The data which the attacker is trying to access is mostly sensitive and confidential information. Most common data breaches are personal information such as password, pin numbers, source code etc, Hackers may also steal network administration and configuration details to exploit a network.

Countermeasure

Encrypt the data. Use key management in order to keep the encryption keys safe. Resource Back-up.

Data Remanence

Data remanence is the retention of deleted data over a storage medium. Data remains even after multiple attempts have been made to delete or remove the date. This makes hackers easier to get data which has not been erased properly in storage. Many files and other data on cloud do not delete immediately when the client requests. It is moved to another location where it makes easy for the client to undo a mistake. Many application and the software automatically backup copies if they are edited. When data keeps replicating it is easier for the intruder to get data from various location even if he fails multiple times.

Countermeasure

Overwriting. Getting service from providers which offer media destruction

Application related Security Threats

Cross-site Scripting

Cross-site scripting referred as XSS is a client-side code injection attack where a hacker executes code which is malicious into a web application. These scripts are mostly in the form of JavaScript code executed by the browser. For example, an attacker may inject a code in a webpage which is vulnerable, the code executes and steals cookies every time the user visits the website. Another scenario of cross-site scripting is attacker injects code in a legitimate webpage and the malicious code redirects to a duplicate page similar to the legitimate webpage where the victim might not be aware of this. The victim will be using the duplicate webpage which steals information like password or pin number where the victim thinks that the webpage is legitimate.

Countermeasures

Use HTTP only cookie flag. Check the URL and user input validation.

Cookie Poisoning

Cookie poisoning is an attack by a hacker trying to access or steal a cookie (a piece of information kept in the browser that keeps the user session information for a site). An intruder also tries to forge a cookie for skipping some of the security parameters in a session. The piece of information in the cookie may contain important data such as password and pin numbers. An attacker can get access to his/her account if the cookie is stolen or manipulated because a cookie can resume a session where it was left from. An example of cookie poisoning is after selecting some items in an online retail e-shopping website where an attacker intercepts and tries to get the cookie before the data is sent to the website server during a "cart checkout" then attacker tries to modify the cost of the items selected during the session.

Countermeasure

Deleting cookies stored in browser regularly. Do not sign up for sites and newsletters that are legitimate.

Cloud Service Provider related Security Threats

Malicious Insider

A disgruntled employee of cloud service provider becomes a malicious insider who has an access to any organization data, network and uses it in a way that confidentiality, integrity, and availability of organization get affected. Affecting monetary value and productivity losses are some of the ways of the malicious insider to affect an operation. Hackers contact insiders of an organization to steal most important data. Valuable data of any organization can give them revenues. Some intruders are just curious to check what kind of data an organization has so they contact insiders to get some of the information. Also, former worker who was

recently stripped of their position gives away the information they know just to take revenge on the cloud service providers.

Countermeasure

Identity and Access management. Log monitoring and analysis. Separation of duties.

Vendor Lock-In

Vendor Lock-In is a scenario where a customer using a service cannot easily transform into a competitors service. Many customers work with the same service providers just to avoid some chaos in their process. It mainly makes a customer dependent on any service or product they need. Customers are mostly worried about the data if their cloud service providers come to know that the customers are transferring to a different service provider. Cloud service providers may hike the price of the service when their contracts come to an end. Customers tend to be scared whether cloud service providers may leak their data and resources due to transformation.

Countermeasure

Select cloud service providers wisely in the first place. Retain ownership of the data and document all the processes.

Network Related Security Threats

Denial of Service

Denial of service is one of the deadliest attacks and even it has ranked as one of the major threats. Attacker searches for some vulnerability in the service offered by cloud and disturbs the service. Attackers simply place as many virtual machines in a network making use of all bandwidth so that other legitimate machines get no service this type of attack is distributed denial of service (DDOS). The attacker basically overloads the system with service request so that it won't be able to reply to any requests and so resource will not be available to any of the users. There are many types of denial of service attacks such as syn floods, UDP floods, ICMP floods, ping of death and smurf attack.

Countermeasures

Deploy an intrusion detection system. Using packet filtering from each host. Monitoring logs.

Domain Hijacking

Domain name hijacking is a theft where an attacker takes full control and access to a domain without the permission of original registrant. This type of attack can also happen due to a security vulnerability in the hosting company. Hijacked domain is basically used for malicious use. Hackers may demand money from the owner of the website to get the website back. In some cases, the website is transformed and used mostly for phishing and other malicious activity. Attackers try to change the ownership to some other name and it is very hard to get the same domain. The attacker may impersonate as the owner and request the domain vendor to transfer the admin rights to some other user. [6]

Countermeasures

Choose a trusted domain provider. To access any configuration settings set up a strong authentication process. Utilize WHOIS privacy.

5. CONCLUSION

Cloud has been providing service to the companies with vast number of option for managing its infrastructure and organization model. It can be a big improvement for all startup companies where this cloud service gives the opportunity to reduce cost in maintaining infrastructure and in administration which is similar to a well-developed company. In cloud, there is no big investment needed to update the services required by the company. Customers have been benefited by cloud service but users have to understand that there are also certain security flaws which can cause more damage to company. Customers have to know about all the threats and risks caused due to cloud service in order to keep the data and other resources safer. Hackers always try to find loop holes in any new technology and the exploit it. Security in cloud has been one of the challenges for cloud service providers. In order to provide better quality of service to cloud user security flaws must be identified and mitigated.

6. REFERENCES

[1] Ramgovind S, Eloff MM, Smith E, 'The Management of Security in Cloud Computing', IEEE, 2010
[2] Leavitt N, 'Is Cloud Computing Really Ready for Prime Time?',IEEE Computer Society ,2009.
[3] Balachandra R K, Ramakrishna P V, Dr. Rakshit A, 'Cloud Security Issues',Modern Education and Computer Science,2009.
[4] Te-Shun Chou,'Security Threats On Cloud Computing Vulnerabilities',Internation Journal of Computer Science and Information Technology,2013.
[5] Kazi Zunnurhain and Susan V. Vrbsky, 'Security Attacks and Solutions in Clouds, 2014.
[6] Rajani Sharma, Rajender Kumar Trivedi, 2014, 'Cloud Computing –Security Issues, Solution and Technologies', Internation Journal of Engineering Research,2016 .
[7] Juhi Chaudhary, Anurag Mishra, 'Cloud Computing Security Issues and Data Encryption Schemes', International Journal of Engineering Development and Research, 2016.
[8] Archana Srivastava, 'A Detailed Literature Review on Cloud Computing', Communications of the Association for Information Systems, 2014.
[9] Rashmi V. Deshmukh, Kailas K. Devadkarb, 'Understanding DDoS Attack & Its Effect in Cloud Environment', Elsevier B.V,2015.
[10] Vidhya.V, 'A Review of DOS Attacks in Cloud Computing', IOSR Journal of Computer Engineering, 201.

