IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CLOUD COMPUTING SECURITY: THREATS AND ITS MEASURES TO CURB THESE SECURITY ISSUES

Dr. Kainaz Bomi Sherdiwala

Assistant Professor
Department of Computer Application
Z.F. Wadia Women's College & N.K. Jhota College of Commerce, Surat, India

Abstract: This paper discusses about various security issues and threats that a company has to face if it doesn't implements security measures properly and strictly when implementing cloud computing technology in their institution. We have stated few security threats for an organization who keeps its data and information on the cloud. Threats like insecure API's, hijacking of accounts, unauthorized access, loss of data and breach of data persists if proper security measures are not taken. Further, we have discussed the measures to be undertaken by an institution to reduce the risk involved in cloud computing. These measures include the use of strong firewall, intrusion detection system (IDS), information-centric security and strong encryption techniques.

Index Terms – Cloud Computing, Security Threats, Measures

I. INTRODUCTION

Cloud computing is the delivery of different resources or services on the Internet. These resources include tools and applications like databases, data storage, software, servers and networking infrastructure. Instead of keeping data and files on a proprietary hard disk or internal storage device, cloud-based technology makes it possible to save them to a remote database. As long as web service is available, it has the accessibility to the data and the software programs. Cloud computing is the best choice for the business organization for a number of reasons like speed, cost savings, increased productivity, performance, efficiency and security.

Cloud security is necessary for the users who are interested about the safety of their data and information stored on the cloud. Generally, they think their data is safer on their own local servers because they feel they have more control on that data. But in reality, data stored on the cloud may be more protected because cloud service providers undertake strict security measures. Data stored on the local storage premise can be more prone to security breaches. Cloud security provides protection of data stored online on the cloud from theft, leakage, and deletion of data. Methods of providing cloud security include firewalls, information-centric security, Intrusion Detection System (IDS) as well as Strong Encryption Techniques.

II. CLOUD SECURITY ISSUES AND THREATS

The latest research shows that around 70 percent of the world's businesses now operate on the cloud with the fact that it provides benefits like lower installation and maintenance costs, greater flexibility, automatic software updates, more collaboration, and the liberty to work from anywhere.

Still, the cloud computing has some issues regarding security. The latest research has showed that majority of organizations are now seriously concerned about the cloud security. Nowadays, almost all the organizations have adopted cloud computing in their business. However, cloud security becomes most essential with the adoption of the cloud computing technology. Here comes the need to ensure that the organization is capable of protecting against the top security threats and challenges to cloud security.

Some of the security concerns for cloud-based services are discussed below:

1. **Insecure API's** - Application Programming Interfaces (API) gives opportunity to the users to customize their cloud experience. However, APIs can become a threat to cloud security due to its behaviour. It provides companies with the ability to customize features of their cloud services according to their business needs. Security risks increases with the increase in the growth of the infrastructure of API. APIs provides tools to the programmers to develop their programs to integrate their applications with other important software.
2. **Hijacking of Accounts** – The problem of accounts hijacking has occurred with the growth and advancement of the cloud technology in many business organizations. The hijackers have the ability to use the client's login credentials to access the sensitive information stored on the cloud. The attackers can even tamper and manipulate information through hijacked data. The use of weak and reused passwords often allows attackers to easily steal credentials.
3. **Unauthorized Access** - The cloud-based deployments are outside the network and can be directly be accessible from the public Internet. While this is a benefit for the employees and customers for easy access to the infrastructure, it also makes it much easier for an attacker to have unauthorized access to the resources of an organization's cloud-based. Improper or weak configured security measures can enable an attacker to gain direct access without any knowledge of the organization.
4. **Loss of data** - Data on cloud platform can be lost through any natural calamity, malicious attack like phishing, spoofing etc or a data accidentally deleted by the service provider. Loss of useful information can be threatful to businesses that don't implement proper recovery measures. Companies like Amazon and Google are examples of an organization that suffered loss of data by permanently destroying data of its own customers.
5. **Breach of Data** – Data Breaching have existed in all forms despite of Cloud computing technology being relatively new. In cloud computing, sensitive and all types of data are stored online rather than on premise. So the question of data being safe arises. After recent surveys, it has been found that data breaching was three times more likely to occur for organisations that implement the cloud than those that don't. It is believed that security measures of organization to protect data on cloud platform are relatively low.
6. **Denial Of Service (DOS) Attacks** - Unlike other type of cyberattacks, which are generally launched to hijack sensitive information, denial of service do not attempt to breach our security boundaries. Instead, they make our website and servers unavailable to the users. However, in some case DoS is also used to slow down security appliances such as web application firewalls.
7. **Lack of Proper Diligence** - Most of the problems arises when an organization is not clear about the plan for its goals, resources, and policies about the cloud. Moreover, insufficient diligence can create a security risk when an organization shifts to the cloud quickly without considering that the services will not be as per customer's expectation.
8. **Exposure of Credentials** - With the increase in use of cloud-based email and document sharing services like Google Drive, OneDrive etc employees have become acquainted with the receiving emails with links which enforces the receiver to click on that link and confirm their account details for gaining access to a particular file or website. This makes the task of cybercriminals much more easier in leaking an employee's credentials for cloud services.

III. NEED FOR CLOUD SECURITY

Cloud security involves the methods and technology that protect cloud computing environments against external as well as internal threats of cyber security. Cloud computing, which delivers information technology (IT) services through the internet, has become mandatory for institutions and governments who are searching for innovations. Cloud security is designed to prevent unauthorized access and to keep data in the cloud secure from emerging cybersecurity threats.

Cloud security or cloud computing security, consists of a set of policies and procedures to protect cloud-based systems and data on the cloud. These security measures are implemented to protect cloud data, customers' privacy as well as setting authentication policies for individual users.

IV. SECURITY MEASURES

1. **Use of Strong Firewall** – Majority of the firewalls are very simple. They generally inspect only the packet's source and destination. Some advanced firewalls does stable packet checking, which examines the integrity of the data packets before accepting or rejecting the packet. Such strict measures are necessary to overcome the most critical threats out there today.
2. **Information-Centric Security** - In order to retain control of data in the cloud, it may be recommended to undertake an approach of protecting data from within the organisation. This technique is known as information-centric security. This technique requires intelligence be kept in the data itself. Data needs to be self-describing regardless of its environment. When accessed, data consults its policy and tries to redefine a secure environment that is considered as trustworthy.
3. **Intrusion Detection System (IDS)** – Number of IT security compliance standards enforces business organisations to implement a system of tracking attempts made by the intruders. Therefore, any business that wants to satisfy their compliance standards, they have to use IDS event logging solutions compulsory. Some cloud providers provide monitoring for IDS, and will constantly revise their security rules for their firewalls to detect threat signals and malicious IP addresses.
4. **Use of Internal Firewalls** – Internal attacks can be blocked or stopped with the help of internal firewalls. Infrastructures that does not support internal firewalls to prohibit access to sensitive information and applications is not considered to be secured. Therefore, internal firewalls that keep individual databases and applications separated, can be helpful in limiting the damage from an attack.

5. **Strong Encryption Techniques** – In order to keep our most sensitive data from being accessed by an unauthorised party, data encryption technique should be applied to the data that is stored on our cloud infrastructure. Strong encryption can decrease the chance of stolen information being used against our company or our clients before we get an opportunity to warn them so they can take preventive steps in advance.

V. CONCLUSION

Despite several benefits provided by the cloud computing, it also encourages security concerns that obstructs the adoption of the cloud computing. All the users whether individual or organization should be aware of the security threats that exists in the cloud. Considering the security threats and its counter measures will help organizations to carry out the cost benefit analysis and will force them to shift to the cloud. As the cloud computing utilizes many traditional along with novel technologies, it possesses conventional as well as unique security issues [11][12].
This paper presents the security issues that arise due to the implementation of the cloud computing paradigm in the business organisation. Subsequently, the measures to be undertaken against these security threats are also discussed.

VI. REFERENCES

1. R. Agrawal, Legal issues in cloud computing, in: IndicThreads.com, Conference on Cloud Computing, 2011.
2. K. Alhamazani, R. Ranjan, K. Mitra, F. Rabhi, S.U. Khan, A. Guabtni, V. Bhatnagar, An Overview of the Commercial Cloud Monitoring Tools: Research Dimensions, Design Issues, and State-of-the-Art, arXiv preprint arXiv:1312.6170, 2013.
3. M. Ali, R. Dhamotharan, E. Khan, S.U. Khan, A.V. Vasilakos, K. Li, A.Y. Zomaya, SeDaSC: secure data sharing in clouds, IEEE Syst. J. 2015.
4. Hewlett Packard, 5 cloud security concerns you must address, Business white paper by Hewlett Packard, No. 4AA3-8247ENW, rev. 1, 2012.
5. Y. Hu, T. Li, P. Yang, K. Gopalan, An application-level approach for privacy-preserving virtual machine checkpointing, in: IEEE Sixth International Conference on Cloud Computing, 2013, pp. 59–66.
6. M. Hussain, H. Abdulsalam, SECaaS: security as a service for cloud-based applications, in: ACM Proceedings of the Second Kuwait Conference on e-Services and e-Systems, 2011, p. 8.
7. A.S. Ibrahim, J. Hamlyn-Harris, J. Grundy, M. Almorsy, Cloudsec: a security monitoring appliance for virtual machines in the iaas cloud model, in: IEEE 5th International Conference on Network and System Security (NSS), 2011, pp. 113–120.
8. W.A. Jansen, Cloud hooks: Security and privacy issues in cloud computing, in: 44th Hawaii International Conference on System Sciences (HICSS), 2011, pp. 1–10.
9. https://www.imperva.com/blog/top-10-cloud-security-concerns
10. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns
11. https://www.whoa.com/5-must-have-cloud-computing-security-features
12. https://www.investopedia.com/terms/c/cloud-security.asp