International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

Security Exposure and Vulnerability Detection in Cloud Computing

Dr. Amanpreet Singh[1], Dr. Rajeev Kumar[2]

[1]IKG Punjab Technical University, Assistant Professor, Jalandhar.
[2]Associate Professor, Teerthanker Mahaveer College of Engineering, Moradabad

---

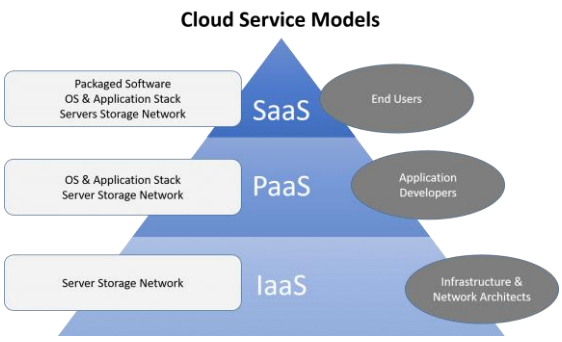
Abstract - *It is an evolution of the IT architecture from centralized computing to network-dependent systems with distributed assets and distributed management responsibilities. Cloud Computing is not a new technology. It is well known for its pay-per-use model for billing customers and other characteristics such as elasticity, ubiquity, scalability and business resource availability.*

Key Words: Cloud Computing, Cloud Security, Cloud Threats, Cloud Vulnerabilities.

1. INTRODUCTION

Cloud computing is a model that allows easy, on-demand network access to a common pool of configurable computing resources, such as networks, servers, storage, applications that can be easily distributed and released with minimal management effort or service provider involvement. Cloud Computing is a distributed architecture centralizes the capital of the system on a flexible basis in order to provide computing resources and facilities on demand. Cloud Service Providers (CSPs) provide cloud platforms for their services. Customers need to use and build their web services, just like Internet service providers deliver high-speed costumers Broadband for Internet access. CSPs and ISPs (Internet services Providers) both provide services.

In general, cloud providers are providing three kinds of services, i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are various reasons for companies to go forward that require cloud storage as it was only necessary to pay for the services on the basis of consumption. In comparative analysis, organizations can effectively address the needs of quickly Moving markets to ensure that they are still at the forefront Added benefit to their customers [1].



Cloud computing tended to be a commercial imperative, impelled by the concept of only utilizing the infrastructure without handling it. While this concept was originally only present in the research sector, it has increasingly been adopted by organizations such as Microsoft, Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new start-ups to enter the market, when the cost of infrastructure is reduced significantly. This helps developers to reflect on market value rather than on the beginning budget. Customers of commercial clouds rent computational resources (virtual machines) or computing data (virtual data) dynamically, depending on the needs of their company [2]. Using this technology, users can access heavy-duty applications through lightweight mobile devices such as cell phones, PCs and PDAs.

2. CRUCIAL CLOUD SECURITY THREATS:

Data breach: The threat of data breach is not exclusive to cloud storage, but regularly positions as a top priority for cloud customers.

Data failure without backup: an accident or incident will lead to an irreversible loss of consumer data unless steps are in place to back up the data.

Account hijacking: using compromised passwords, criminals can obtain access to sensitive areas of cloud computing systems, undermining the security, security and availability of those systems.

Insecure APIs: As the public "front door" to your programme, the API is likely to be the primary entry point for hackers. Using pen analysis to discover the security flaws of the APIs you are using. [3]

Network-sniffing: is an offence in which unencrypted data is hacked across the network as an attacker who can crack passwords that are not adequately encrypted through contact. To reduce this form of attack, use encryption methods to protect the data. [4]

Side-Channel-Attaches: Attacker may attempt to damage the cloud by putting a malicious virtual machine in located close to a cloud server target and then triggering a side-channel attack.

Man-in-the-Middle Attack: where the attacker positions himself between two clients, this form of attack happens. The contact groups are not aware of the attacker. The hacker will change the original data. [6]

SQL-Injection attack: is a special form of threat in which a hacker uses a special sort of character, such as a statement with a value of 1=1, to return the desired result since it is always valid.

Failure to notify: Service Provider unavailability, Failure of data link, Non-delivery of communications, Unintended out-of-sequence delivery, Unintended interruption of delivery, Accidental denial of service. The Internet does not have a consensus about the quality of operation. There are no promises as to how long a message would take to get to the receiver, or even if it will actually get there.

Port-filtering: Port checking is utilized by programmer as Port 80(HTTP) which is consistently accessible to give web administrations to the customers [5]. A few ports are not opened constantly they will open just when they are required in this manner the ports be made sure about by encryption. To diminish this kind of assault use firewalls.

Accidental Misrouting: the danger of accidental misrouting entails the possibility that the information could be sent to an incorrect address as it is transmitted over a network.

Communication infiltration: This threat includes the following categories of events: breaking into a device that uses buffer overflow attacks, masquerading as a website, masquerading as an established commercial application customer, masquerading as a new e-commerce application user, denial of service (deliberate), flaming threats, and spamming.

Malfunction to inform: Service Provider unavailability, Failure of data link, Non-delivery of communications, Unintended out-of-sequence delivery, Unintended interruption of delivery, Accidental denial of service. The Internet does not have a consensus about the quality of operation. There are no promises as to how long a message would take to get to the receiver, or even if it will actually get there. [7]

3. PROTECTION AND REGULATORY POLICY:

The security strategy rules aligned with the vulnerability and security measures referred to the above shall be followed.

1. **Identification and verification:** Users must be marked using a special UID that must be protected.
2. **Logical access control:** In order to minimize the possibilities for an unauthorized party to exploit accounts as part of an attack, user accounts must be established in compliance with the security standards of need-to-know access, least privilege and division of duties.
3. **Efficient Data Management:** Data stored in the cloud has its own rules for data integrity and security. The benefits of using cloud data management include consolidation of processes such as backup, disaster recovery, archiving and analytics, and cost savings.
4. **Recording actions / events and avoidance of interference:** any occurrence, accident, interference or malfunction of hardware or / and software functions must be reported and the proper response mechanism must be in place.
5. **Handling protection accidents:** a protocol for disclosing errors and general safety accidents is mandatory. Recorded protocols should be in order to ensure a prompt and efficient response to the event of a safety incident. [8]
6. **Access control and usage of resources:** Access / usage privileges should be given in compliance with user responsibilities and must be decided via a comprehensive registration process. [9] Usage of services, apps should be controlled by the teams and must conform with the position of the customer.
7. **Compliance with regulatory requirements:** Compliance with the current legal and regulatory system is important. Track both legal and legislative criteria and evaluate how they can be satisfied.
8. **Monitoring and Control:** Audit records and case reports must be reported to help the detection of violations or attempted violations and the documentation of any suspected events. It can entail the use of special software to handle and track records, report device errors, restart, adjust access privileges, event logs, files accessed, etc.

4. CONCLUSIONS

While cloud computing may be seen as a revolutionary phenomenon that is going to revolutionize the way we use the Internet, there is a great deal to be careful about. However, we must be quite vigilant to consider the security threats and problems raised by the use of these technologies. Cloud computing is no exception to this. Key security issues and problems currently facing cloud infrastructure are outlined in this article. Cloud infrastructure has the potential to become a leader in supporting a stable, decentralized and economically viable IT solution in the future.

REFERENCES

[1] S. B. Yadav, and D. Tianxi, "A Comprehensive Method to Assess Work System Security Risk," Communications of the Association for Information Systems: Vol. 34, Article 8, 2014.

[2] A. Kundu, C. D. Banerjee, P. Saha, “Introducing New Services in Cloud Computing Environment”, International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[3] D. A. B. Fernandes, L. F. B. Soares, J. V. Gomes, M. M Freire and P. R. M. Inácio, "Security issues in cloud environments: a survey", Int. J. Inf. Secur. 13:113–170, 2014.

[4] B. R. Kandukuri, R. V. Paturi and A. Rakshit, “Cloud Security Issues,” 2009 IEEE International Conference on Services Computing, Bangalore, India, September 21-25, 2009. In Proceedings of IEEE SCC'2009. pp. 517-520, 2009. ISBN: 978-0-7695-3811-2.

[5] Aman Bakshi, Yogesh B. Dujodwala, “Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine,” ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[6] Gai, Keke, Meikang Qiu, and Sam Adam Elnagdy. "A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance." Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on. IEEE, 2016.

[7] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[8] Fazio, Maria, et al. "Big data storage in the cloud for smart environment monitoring." Procedia Computer Science 52 (2015): 500-506.

[9] K. Kaur, "A Review of Cloud Computing Service Models", International Journal of Computer Applications, Vol.140, No.7, pp.15-18, 2016.

[10] Liu Y Wang Lunyan, Hu Fangyuan, Yuan Lu. Security AccessControl in SaaS Mode Based on Improved RBAC Model [J] .Modern Computer, 2017 (15): 81-84.

[11] Teli, Prasad, Manoj V. Thomas, and K. Chandrasekaran. "Big Data Migration between Data Centers in Online Cloud Environment." Procedia Technology 24 (2016): 1558-1565.