Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

27

Cloud Computing Security Issues and Existing Solutions

Vasisth Roy

Department of Computer Science and Applications, Dr Vishwanath Karad MIT World Peace University – Pune

1132210684@mitwpu.edu.in

Chaitanya Deshpande

Department of Computer Science and Applications, Dr Vishwanath Karad MIT World Peace University – Pune

1132210400@mitwpu.edu.in

Nikesh Kumar

Department of Computer Science and Applications, Dr Vishwanath Karad MIT World Peace University – Pune

1132210102@mitwpu.edu.in

Dr. Mahendra Suryavanshi

Department of Computer Science and Applications, Dr Vishwanath Karad MIT World Peace University – Pune

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Abstract

Cloud computing benefits both the service providers and end-users by offering enhanced accessibility, reduced IT maintenance burdens, scalable infrastructure, and cost-effective services. Cloud computing technology has several issues such as security, service reliability, vendor lock-in, data lock-in, load balancing, in cast, lack of transparency, resource allocation, interoperability. Security issues in cloud computing arise due to several parameters such as the shared infrastructure, weak access controls, data confidentiality, integrity, availability, and compliance with regulations. In this paper, existing solutions to mitigate cloud security issue are analyzed.

Index Terms- cloud computing, security, performance, issues

I. INTRODUCTION

Cloud computing is a technology that provides servers, storage, databases, software, and networking resources over the internet. Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) are the three service models of cloud computing. Public, private, and hybrid cloud are the cloud deployment models. Public cloud services are provided by third-party cloud providers, while private cloud services are operated by a single organization. Cloud computing services are provided through large data centers. Cloud data centers are categorized into switch-based, server-based and hybrid out of which switch-based data center networks are large scale high performing data center networks [12, 13, 14]. According to market research, the global cloud services market was estimated to have a value of $551.8 billion in 2021 and is expected to grow at a compound annual growth rate (CAGR) of 16.6% from 2022 to 2031 [1, 11].

Cloud computing eliminates the need to invest in physical computing infrastructure. It reduces capital expenses, making it a cost-effective solution. Measured services, rapid elasticity, resource pooling, broad network access, on-demand self-service are the five properties of cloud computing. Cloud computing benefits both the industry and end-users by offering enhanced accessibility, reduced IT maintenance burdens [11].

Cloud computing presents several issues including security concerns, data privacy, service reliability, vendor lock-in, data lock-in, load balancing, in cast and lack of transparency,

resource allocation, interoperability [6, 7, 8, 9, 10]. The cloud requires users to entrust their data and applications to third-party providers, raising concerns about data security and privacy. Additionally, cloud providers can experience service disruptions or outages, leading to significant impacts on users. Security and privacy remain major concerns for organizations considering cloud adoption, with data breaches, data loss, and confidentiality breaches being some of the most cited issues [2]. Finally, cloud providers may not provide sufficient information about how their systems work, which can make it challenging to assess their reliability and security. In this paper, authors have reviewed security challenges in cloud computing environment. Section 2 describes impact of security issue on cloud providers and users. Existing solutions to cloud security are reviewed in section 3. Section 4 analyses existing work on cloud security. Finally, paper is concluded in section 5.

II. SECURITY ISSUES IN CLOUD COMPUTING

Security issues in cloud computing refer to the risks associated with protecting data and systems in the cloud. Due to the sharing of resources among multiple users, potential security vulnerabilities arise, and data breaches, unauthorized access, and data loss may occur. Cloud security is still a major concern for organizations, and despite the significant efforts made by cloud providers to improve their security measures, many challenges still exist such as data confidentiality, integrity, availability, and compliance with regulations. Selecting a trustworthy and reliable cloud provider is crucial since providers are responsible for securing their systems and protecting user data [3].

Security issues in cloud computing arise due to several parameters, such as the shared infrastructure, which involves the sharing of resources among multiple users and can create potential security vulnerabilities. Data breaches pose another significant security risk, resulting in the loss, theft, or unauthorized access of data. Other parameters such as weak access controls, data confidentiality, integrity, availability, and compliance with regulations can also create security issues in cloud computing. It is crucial for cloud providers to implement robust security measures to protect their infrastructure and customer data and for users to ensure that they use secure practices when accessing and storing data in the cloud [4].

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

III. EXISTING SOLUTIONS FOR THE CLOUD SECURITY ISSUE

The following are some solutions proposed by researchers to address security issues in cloud computing: encryption to protect data, access controls to prevent unauthorized access, security monitoring to detect and respond to incidents in real-time. Additionally, compliance automation, disaster recovery planning, and trusted computing technologies are suggested to further enhance cloud security. It is essential for cloud providers and users to implement these solutions effectively and continuously monitor and improve their security posture to stay ahead of emerging threats.

3.1 Encryption:

Researchers have proposed using encryption to protect data in transit and at rest. End-to-end encryption can be used to ensure that data remains secure even if it is intercepted during transmission. It converts plaintext data into ciphertext using an encryption algorithm and a secret key, which can only be decrypted by authorized parties who possess the key. Data-at-rest encryption can be used to protect data that is stored in the cloud. Encryption keys can also be managed by the user to ensure that only authorized parties can access data [15].

3.2 Access Controls:

Access controls are essential for preventing unauthorized access to cloud resources Access controls can be implemented at various levels of the cloud infrastructure, including physical, network, host, and application layers. They can also be used to enforce security policies, such as authentication, authorization, and auditing. Effective access controls can help prevent unauthorized access to cloud resources, reduce the risk of data breaches, and ensure compliance with security and privacy regulations [16].

3.3 Security Monitoring:

Security monitoring can help detect and respond to security incidents in real-time. Researchers have proposed using machine learning algorithms and other advanced analytics techniques to improve security monitoring. These tools can help identify patterns and anomalies in user behavior, network traffic, and system activity that may indicate a security breach. Advanced analytics techniques like machine learning and

artificial intelligence can boost security monitoring by identifying abnormal behavior and patterns that may indicate security threats. Nevertheless, security monitoring in cloud environments poses several challenges, including ensuring compliance with data privacy regulations and facilitating effective communication between security teams and cloud providers [5].

3.4 Compliance:

Cloud providers need to comply with various regulations and standards, and researchers have proposed using automation tools to ensure compliance and reduce the risk of non-compliance. These tools can automate compliance monitoring, reporting, and auditing, and can help identify and remediate compliance issues before they become a problem.

3.5 Disaster Recovery:

Disaster recovery planning is critical to ensure that data and services are available in case of a disaster. Researchers have proposed using redundant systems, failover mechanisms, and data replication to improve disaster recovery. Redundant systems involve duplicating critical components to ensure that if one fails, there is another to take its place. However, effective DR in cloud environments requires careful planning, testing, and monitoring, as well as coordination between cloud providers and customers to ensure that recovery objectives are met. Failover mechanisms involve automatically switching to a backup system in the event of a failure. Data replication involves copying data to multiple locations to ensure that it is available in case of a disaster [17].

3.6 Multi-factor authentication:

With multi-factor authentication, users must authenticate using several different methods to access cloud resources. This often entails a mix of something the user is, something they have, or something they know (such as a password, token, or smart card). (e.g., biometric data). MFA adds an additional layer of protection and makes it more challenging for attackers to get unauthorized access to cloud services by demanding multiple forms of authentication [18].

3.7 Virtual Private Network:

The establishment of a secure and encrypted connection between a user's device and the cloud environment is done using a virtual private network (VPN). This method makes sure that data is secure and cannot be intercepted by unauthorized persons while it is in transit. A user's device establishes a secure tunnel to the cloud environment when they connect to it using a VPN, ensuring that data is encrypted and cannot be accessed by unauthorized parties. However, VPNs may introduce performance and scalability issues, and may not be well-suited to highly distributed cloud environments. It can help protect against interception and eavesdropping of sensitive information during transmission and can also be used to enforce access controls and authenticate user identities [19].

3.8 Network segmentation:

The act of segmenting a network into smaller, more secure subnetworks or segments is known as network segmentation. Network segmentation can assist in preventing attackers from moving laterally through the network if they get access to one portion of it by isolating various parts of it. By dividing the network into smaller, isolated segments, organizations can apply different security policies and controls to each segment based on the risk profile and access requirements of the applications and data hosted in them. Network segmentation can be used in a cloud computing environment to establish distinct network segments for various cloud resources, such as databases, applications, and web servers [20].

IV. ANALYSIS AND DISCUSSION

There are three different approaches to deal with security issues in cloud computing environment. First, is to prevent security threats at first place only. Second, continuously monitor and detect security breaches in cloud computing environment. Third, recover the target environment from security attacks after detecting security threats on the cloud environment.

Encryption to overcome cloud security issue is considered as an effective and efficient technique as it is required to be implemented at application layer only. Access control mechanism is implemented at all layers that is physical, link, network, transport and

application layer of TCP/IP protocol suit. Due to this, access control mechanism is considered as robust to ensure security in cloud environment.

Researchers have proposed using redundant systems, failover mechanisms, and data replication to improve disaster recovery. Multi-factor authentication is one of the important techniques to ensure robust security in cloud environment as multiple forms of authentications are required for attackers to get unauthorized access to cloud resources.

V. CONCLUSION

Cloud computing enables service providers to offer computing services over the Internet. These services include storage, servers, networking, applications and many more. Cloud computing is considered as an eminent model that allows cloud users to access vast set of cloud services with minimum efforts and cost. Security issues in cloud computing refer to the risks associated with protecting data and systems in the cloud. There are various security threats to cloud security such as hypervisor vulnerability, VM escape, injection attack, cross-site scripting, DNS poisoning and phishing, DoS attack. Security attacks on cloud resources are avoided through encryption, access control, security monitoring, disaster recovery, multi-factor authentication technique. The multi-factor authentication is considered as an efficient and robust technique to ensure security of cloud resources. Still further research endeavors are required to enhance applicability of multi-factor authentication.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to Dr Vishwanath Karad MIT World Peace University for providing the necessary resources and support for this research. We are also grateful to Dr. Mahendra Suryavanshi for his valuable guidance and support throughout the research process.

We would like to thank the participants who generously contributed their time and information to this study.

Finally, we would like to acknowledge the contributions of all the individuals who helped make this research a success. Without their support and encouragement, this research would not have been possible.

REFERENCES

1. Kashinath G, Vineet K: Cloud Services Market (2023) **Link**
2. Botta, A., de Donato, W., Persico, V., & Pescapé, A.: Integration of cloud computing and internet of things: a survey. (2016) Link
3. Almorsy, M., Grundy, J., & Müller, I: An analysis of the cloud computing security problem. (2016) Link
4. Rittinghouse, J. W., & Ransome, J. F. Cloud computing: implementation, management, and security. (2016)
5. V. Swathi, Dr. M. P. Vani: Security and Privacy Challenges in Cloud: Survey and Research Directions. (2017) Link
6. Fox, Armando, Rean Griffith, Anthony Joseph, Randy Katz, Andrew Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, and Ion Stoica. "Above the clouds: A berkeley view of cloud computing." Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS 28, no. 13 (2009): 2009.
7. A Vouk, Mladen. "Cloud computing–issues, research and implementations." Journal of computing and information technology 16, no. 4 (2008): 235-246.
8. Tiwari, Pradeep Kumar, and Bharat Mishra. "Cloud computing security issues, challenges and solution." International journal of emerging technology and advanced engineering 2, no. 8 (2012): 306-310.
9. Ghanam, Yaser, Jennifer Ferreira, and Frank Maurer. "Emerging issues & challenges in cloud computing—a hybrid approach." (2012).
10. Suryavanshi, Mahendra, Ajay Kumar, and Jyoti Yadav. "An application layer technique to overcome TCP incast in data center network using delayed server response." International Journal of Information Technology 13 (2021): 703-711.
11. Sriram, Ilango, and Ali Khajeh-Hosseini. "Research agenda in cloud technologies." arXiv preprint arXiv:1001.3259 (2010).

12. Al-Fares, Mohammad, Alexander Loukissas, and Amin Vahdat. "A scalable, commodity data center network architecture." ACM SIGCOMM computer communication review 38, no. 4 (2008): 63-74.
13. Yao, Fan, Jingxin Wu, Guru Venkataramani, and Suresh Subramaniam. "A comparative analysis of data center network architectures." In 2014 IEEE International Conference on Communications (ICC), pp. 3106-3111. IEEE, 2014.
14. Suryavanshi, M. M. "Comparative analysis of switch-based data center network architectures." J Multidiscip Eng Sci Technol (JMEST) 4, no. 9 (2017): 2458-9403.
15. Duan, L., Yan, Z., Zhang, X., & Ruan, L. (2013). "A Review on Encryption Techniques in Cloud Computing." In Proceedings of the 2013 International Conference on Cloud Computing and Big Data (pp. 16-21).
16. Liao, Y., Ren, K., Guo, J., & Li, X. "Access Control in Cloud Computing: A Survey." IEEE Access, 7, 541-557. (2019).
17. Goyal, M. & Singh, R. "A Comprehensive Study of Security Issues and their Countermeasures in Cloud Computing." Journal of King Saud University - Computer and Information Sciences (2020).
18. Kshetri, N., & Voas, J. "Security and privacy in cloud computing: vision, trends, and challenges." IEEE Cloud Computing (2016)
19. Li, X., Wang, B., Zhou, X., Sun, S., & Zhang, Y. "A review on cloud security." Journal of Ambient Intelligence and Humanized Computing (2021).
20. Kaur, H., & Goyal, A. "Cloud computing security: A comprehensive review." International Journal of Advanced Research in Computer Science. (2021)