RESEARCH ARTICLE | JUNE 03 2024

Securing the cloud: An in-depth review of security threats in cloud computing

Palnati Neha Reddy

AIP Conf. Proc. 3112, 020025 (2024)
https://doi.org/10.1063/5.0211819

Securing The Cloud: An In-Depth Review of Security Threatsin Cloud Computing

Palnati Neha Reddy[1, a)]

[1]*Vellore Institute of Technology, Vellore, Tamil Nadu, India*

[a)] *Corresponding author: nehareddy4402@gmail.com*

Abstract. These days, cloud computing is an essential component of contemporary technology, providing advantages including cost reduction, scalability, and flexibility. But as more businesses use cloud computing, worries about security risks have also grown. Because a security breach might jeopardise sensitive data and information, cloud computing security is an important concern. Organisations need to be vigilant and aware of the many security risks related to cloud computing in order to guarantee the protection and security of their data on the cloud. This analysis will examine the many security issues that cloud computing encounters and provide solutions to reduce the associated risks. Organizations may protect their data in the cloud by being aware of possible security risks and putting in place strong security procedures.

Keywords:- CC, DDoS, SS and IDEA

INTRODUCTION

With its many advantages, cloud computing is an incredible innovation that has captured the interest of technologists all over the globe. Due to growing needs, cloud computing (CC) has received a lot of attention lately. Businesses may gain from cost-effectiveness, worldwide accessibility with reliable internet connection, and better IT administration by using cloud-based storage solutions. The biggest development is cloud computing, which focuses on lowering expenses, decreasing equipment, and offering services. Access to the cloud is possible from any location and it is managed remotely. But crucial data kept on the cloud might be accessed by unauthorised people, which could lead to vulnerability. To solve this problem, specific encryption technology for data security is used. A number of things may lead to cloud security issues, such as system vulnerabilities, unauthorised access, insecure interfaces, and APIs. However, since data may be shared among several persons, detecting illegal behaviour might provide challenges. It is essential to have audit tools that are legally obligated to factual analysis in order to tackle these difficulties. For the purpose of recovering lost or fragmented data, a trustworthy data recovery system should also be in place. Having a cyber-attack-resistant, robust infrastructure is equally important. In today's world of intense computing services that need optimum solutions, cloud security is an important problem. Large firms like to rent technology rather than own it, which is why they overpay for hardware, software, and data storage. This is because cloud computing makes this possible.

RELATED WORK

Now more than ever, the best way to improve cloud security is essential. The biggest concerns to data security and network security in cloud systems have been thoroughly examined and assessed by several individuals. It indicates that virtualization introduces more software to the network system, which, if not developed and implemented correctly, might have a severe influence on security. Information and computer networks must be kept secure by providing services like integrity, confidentiality, authentication, and availability. Cloud Computing (CC) raises several security dangers and concerns in addition to providing a number of helpful features. Because so much data is

International Conference on Contemporary Challenges in Science, Engineering, and its Applications
AIP Conf. Proc. 3112, 020025-1–020025-6; https://doi.org/10.1063/5.0211819

being kept in the cloud and sent via networks, bad actors may take advantage of a number of

weak points. Multiple service-level agreements are covered by security policies, which are developed in accordance with legal standards. Data availability and accessibility must always be guaranteed by cloud providers. Different levels of security are included into different forms of cloud computing (CC), including community, private, public, and hybrid clouds. This allows for numerous steps of data authentication. Using forensic virtual machines and various encryption techniques, data security, privacy, integrity, and trust are preserved. Three types of CC layers exist: CC expansion models that include public, private, community, and hybrid cloud; CC expansion models that include public, private, community, and hybrid cloud; and CC expansion models that only include public cloud. In the healthcare industry, precautions are made to prevent the public disclosure of sensitive patient information. A cloud computing-based healthcare information system has been proposed, which would enable cloud platforms to link hospitals, patients, and health centres while guaranteeing data security and doing away with the need for outside monitoring. Patients and doctors may both access and add data to a single cloud-based database using this technology. An International Data Encryption Algorithm (IDEA) and RSA Security are used in a Web Cloud Encryption Algorithm that has been proposed to improve the security and efficiency of the system by protecting data transmission from healthcare providers to the cloud. Through the use of RSA algorithms for E-health care systems, this invention aims to increase system efficiency in cloud settings and guarantee the security and effectiveness of data transfer from healthcare providers to the cloud. With the use of technologies that can be expanded as required, cloud computing makes it possible for almost anybody to serve as many people as necessary. IaaS, PaaS, and SaaS are among the several services that cloud computing offers. IaaS gives users access to the full range of cloud computing capabilities, such as networking, data storage, and processing power. Networking, storage, and server infrastructure are all included in PaaS.

SECURITY ISSUES AND CHALLENGES

Any organisation must take note of the security risks posed by cloud computing. A business must make the necessary plans and be informed about the dangers, threats, and weaknesses that might arise. Cloud computing's delicate design has given rise to a number of security problems. As a result, it is critical to evaluate cloud networks in order to find specific security threats and vulnerabilities. This entails evaluating weak points and possible assaults in addition to figuring out appropriate ways to improve security and privacy in cloud environments. Such assessments are necessary for cloud computing to be widely adopted. Widget-based apps, open-access commercial online banking portals, and other applications are major uses in banking and e-commerce.

E-commerce is not immune to risks, however; theft, fraud, and security lapses may happen accidentally, on purpose, or as a result of human mistake.
The most common security risks in online shopping are

1. Electronic Payment Systems: Risks include the potential for financial losses, illegal access to private information, and disruptions to the smooth operation of the payment system.

2. E-cash: Since e-cash is a virtual money that is prone to theft, double-spending, and counterfeiting, using it might come with security issues. These hazards have the potential to be financially damaging and raise questions about the payment system's dependability.

3. Abuse of Data: Abuse of data may result in financial fraud, identity theft, and illegal access to private information, among other security risks. These risks have the potential to cause serious harm, including monetary loss and reputational damage.

4. Credit/Debit Card Fraud: This refers to the fraudulent use of another person's credit or debit card to make purchases or get cash.

Some of the other assaults may include

5. Data mining: Security may be jeopardised and a breach may result when private data is used or obtained in a

cloud environment. Customers lose tangible items when their data is kept on the cloud.

control over their data, and cloud service providers may access their private data. Data mining is another option that might lead to a security vulnerability.

6. Distributed Denial of Service (DDoS) Attacks: The goal of a DDoS assault is to overwhelm a server or network with a large volume of traffic coming from many sources, making it unusable for users.

7. Data Structure Attack: Using flaws in a data structure's design or implementation, an attack on a data structure may be used to acquire unauthorised access to private information or carry out destructive operations.

8. Injection: An injection attack is a kind of cyberattack where the attacker infiltrates a programme with malicious code or instructions in order to take advantage of any vulnerabilities and gain unauthorised access to data or system resources.

9. The Exploitation of Authentication: This is the process by which someone gets unauthorised access to a system or network by avoiding or navigating authentication measures.

10. Resource manipulation: This kind of cyberattack involves the alteration or manipulation of system resources by the attacker in order to get unauthorised access or harm a targeted system or network.

11. Phishing: Phishing is the practise of deceiving people into disclosing private information, such as passwords or credit card details, by sending them phoney emails or texts.

12. Malware Infiltration: The uninvited introduction of malicious software into a computer network or system may result in serious consequences including decreased efficiency, system failures, and the pilfering of private information.

13. Attacks connected to authentication: These are malevolent attempts that exploit gaps in the authentication procedure in order to gain unauthorised access to a system.

14. Man-in-the-Middle Attack: A hostile cyberattack known as an MITM attack occurs when an unauthorised person eavesdrops on a conversation between two parties in order to steal private information or assume the identity of one of them. This is achieved by the attacker surreptitiously listening in on, changing, or interfering with the conversation.

Multi-tenancy, or the sharing of physical or virtualized software resources across many separate customers and organisations, presents security concerns. Examples of these resources include organisational memory, hard disc data, grid traffic, hardware measurements, and display shields. In order to satisfy clients' fluctuating resource needs, cloud providers use a service agreement-governed dynamic delivery system consisting of several virtual machines. Nevertheless, a number of regulatory obstacles must be overcome in order to provide low-risk cloud services. Among the advantages made possible by cloud computing are the capacities to lease many resources and virtualize resources. However, risks including system failures, security threats, and other security concerns might appear both inside and outside throughout the cloud infrastructure process. Via firewall breaches or the exploitation of software flaws, attackers may still access cloud systems. This is a serious breach in cloud security that may allow private information, including bank account details, to be stolen. Attackers may get access to infrastructure and steal data via manipulating data, engaging in phishing and fraud, and using software exploitation techniques. Because these assaults use sophisticated methods like as phishing, network penetration, direct hacking, and abusing programming interfaces, they are difficult to identify.

The majority of breaches involving cloud services are caused by malware, insider threats, human mistake, shoddy credentials, or unlawful activities. Attackers with malicious intent, especially those with state sponsorship, use vulnerabilities in cloud service security to steal confidential information from target organisations' networks for financial gain or other illicit uses. Making sure data is secure is one of the main considerations when moving to

eLearning platforms. The data and software are kept on servers that might crash or disappear at any time. Passive security vulnerabilities may happen when a lot of people

access courses at different times and from different places. Fraudsters in the banking sector may design fictitious websites that mimic bank interfaces in an attempt to fool consumers into divulging their login details. They could also con people and get their personal data by sending spam emails and texts. ATMs may have skimming devices connected to them to record users' PINs and account details, which can then be used to conduct business or reset passwords. Additionally, by flooding databases and systems with many queries and transactions, attackers might impede banking operations and provide an opening for Distributed Denial of Service (DDoS) assaults.

SOLUTIONS

While network and data security have become major safety issues in recent years, cloud computing has shown to be quite beneficial for both consumers and enterprises. These advantages include instant scalability, automatic multi-tenancy, virtual presence, and easily accessible resources, applications, and services. Performance is always a crucial factor in a real-world digital application, and security is advantageous if administrators and consumers are aware with the performance statistic. Many approaches have been investigated in an effort to create a cloud system that is safe, dependable, private, and affordable. Businesses that have procedures and policies in place for security and compliance are in charge of safeguarding their company assets and intellectual property. Network indexing, file interpretation, analysis, and log investigation may all be facilitated by the use of digital forensics methods, such as forensic digital toolboxes.
Understanding data security protocols is crucial when using a cloud system with different tenants. It is recommended to use hardware security modules, or HSM modules, for key storage. Services like SaaS, PaaS, and IaaS are available to cloud consumers. For electronic data, the National Institute of Science and Technology stresses the need of encryption and decryption that complies with AES.

Over time, AES has been shown to function better than other cyphers such as RC2, Blowfish, and RC6, notably for a variety of data formats including pictures.

1. Disaster Recovery: In IT platforms, disaster recovery is a major difficulty, particularly in cloud computing, where service providers are required to keep up service to customers even in the event that a calamity shuts down their data centre. To address cloud security concerns, a strong encryption solution was also suggested.

2. Identify-based Encryption: Identify-based encryption, a subset of Advanced Encryption (IBE), provides attribute-based encryption (ABE) and KP-ABE feature-based encryption as its two main ciphertext approaches. An algorithm known as ABE is affected by a certain property, such "location" or "account type," and it influences an individual's private key as well as any encryption techniques used. Assume that the cypher (CP-ABE) cannot be deciphered and that the primary characteristics of the client match the cypher.

3. RSA method: RSA is a popular public-key encryption method that can decrypt encrypted data without the need for a secret key. Because it can detect risks, take appropriate action, stop data breaches, and identify administrators, RSA Security is a powerful defence against computer hackers.

4. Blowfish: With a bit size range of 32–448 bits, Blowfish is an asymmetric black chip that may be used both domestically and internationally in lieu of DES for drop encryption. As a general-purpose algorithm, Blowfish was developed to get over the drawbacks and restrictions of existing algorithms, such as DES and Ageing. The most popular lightweight encryption algorithms for Internet of Things (IoT) devices are RSA and Blowfish, with Blowfish being much quicker than AES.

5. Triple Data Encryption: To protect data in cloud settings, a number of strong encryption methods are used. Triple Data Encryption Standard is one such approach that makes use of a bigger key size in order to improve encryption and guarantee optimal security. Both the Internet of Things and cloud computing

(IoT) are vulnerable to security threats and reliant on one another. It is the client's obligation to secure their data.

6. Virtual Private Network: Encrypting data sent between the organisation and the cloud is advised; this may be done by using a Virtual Private Network (VPN). VPNs provide many encryption levels to protect user privacy. They are particularly helpful for distant work. As an alternative, users may use any third-party encryption programme to encrypt their data before uploading them to the cloud.

7. Security Measures: To stop unwanted access to servers, a number of security measures may be put in place, including SMS authentication, ACL mechanisms, and biometric systems. To keep servers secure, users should get security updates and utilise an SSH key on a regular basis. Access may also be restricted to certain people by using encryption. Applications that are not updated and maintained might expose networks. Microsoft's technology checks and aggregates app updates on a regular basis using a security analyst. Creating and upgrading cybersecurity plans and cyberspace regulations should be a top priority for governments. Recuperation times may be accelerated by putting catastrophe recovery strategies into action in one place.

CONCLUSION

In the next years, cloud computing is anticipated to have a major impact on the economy. Many advantages come with cloud computing, including cost-effectiveness, worldwide accessibility, and effective IT administration. It also poses serious security issues, which need to be handled. Unauthorised access to confidential data kept in the cloud may lead to vulnerability. A number of things, such as staff carelessness, insecure interfaces, APIs, and system flaws, might raise questions about cloud security. Specialised encryption technology, audit tools for factual analysis, a reliable data recovery mechanism, and a robust infrastructure that can survive cyber-attacks are essential for improving cloud security. The most common security risks in e-commerce, such as credit/debit card fraud, e-cash, electronic payment systems, data misuse, and many more, pose a significant risk to the business. In general, in order to improve safety and privacy in the cloud environment, businesses must make the necessary plans and be aware of any possible risks, threats, and vulnerabilities.

ACKNOWLEDGMENTS

I would like to acknowledge my own contributions in conducting this review. I conducted in-depth research, looked at relevant literature, and synthesized the results to produce this comprehensive review. I am grateful for the opportunity to undertake this study and contribute to the field of engineering.

REFERENCES

1. Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloudcomputing in banking and e-commerce and related security threats. Materials Today: Proceedings, 51, 2172- 2175.
2. Bella, H. K., & Vasundra, S. (2022, January). A study of security threats and attacks in cloud computing. In 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 658-666). IEEE.
3. Ahmad, S., Mehfuz, S., & Beg, J. (2022). Assessment of potential security threats and introducing novel data security model in cloud environment. Materials Today: Proceedings.
4. Dhanalakshmi, G., & George, V. S. (2022). Security threats and approaches in E-Health cloud architecture system with big data strategy using cryptographic algorithms. Materials Today: Proceedings, 62, 4752-4757. R.Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
5. Karmakar, A., Raghuthaman, A., Kote, O. S., & Jayapandian, N. (2022, April). Cloud computing application: Research challenges and opportunity. In 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) (pp. 1284- 1289). IEEE.
6. Vashishtha, M., Chouksey, P., Rajput, D. S., Reddy, S. R., Reddy, M. P. K., Reddy, G. T., & Patel, H. (2021). Security and detection mechanism in IoT-based cloud computing using hybrid approach.

International Journal of Internet Technology and Secured Transactions, 11(5-6), 436-451.
7. Ahmad, S., Mehfuz, S., & Beg, J. (2021). Enhancing security of cloud platform with cloud access security broker. In Information and Communication Technology for Competitive Strategies (ICTCS 2020) Intelligent Strategiesfor ICT (pp. 325-335). Springer Singapore.
8. Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.
9. Dhanalakshmi, G., Asha, S. M. R., Dharani, R., Rajeswari, V., & Gobinath, M. (2021). Securing an E-Health Care Information Systems on Cloud Environments with Big Data Approach. Design Engineering, 6986-6994.
10. Das, M., & Dash, R. (2021). Role of cloud computing for big data: A review. Intelligent and Cloud Computing:Proceedings of ICICC 2019, Volume 2, 171-179.
11. Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. Automation in Construction, 122, 103441.
12. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493- 9532.
13. Kunal, S., Saha, A., & Amin, R. (2019). An overview of cloud-fog computing: Architectures, applications withsecurity challenges. Security and Privacy, 2(4), e72.
14. Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy preserving challenges of e- health solutions in cloud computing. IEEE access, 7, 74361- 74382.
15. Rashid, A., & Chaturvedi, A. (2019). Cloud computing characteristics and services: a brief review. InternationalJournal of Computer Sciences and Engineering, 7(2), 421-426.
16. Heidari, A., & Jafari Navimipour, N. (2022). Service discovery mechanisms in cloud computing: a comprehensive and systematic literature review. Kybernetes, 51(3), 952- 981.
17. Mansouri, N., Ghafari, R., & Zade, B. M. H. (2020). Cloud computing simulators: A comprehensive review. Simulation Modelling Practice and Theory, 104, 102144.
18. Domingo-Ferrer, J., Farras, O., Ribes-González, J., & Sánchez, D. (2019). Privacy preserving cloud computing on sensitive data: A survey of methods, products and challenges. Computer Communications, 140, 38-60.
19. Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. IEEE Internet of Things Journal, 8(8), 6222-6246.
20. Helali, L., & Omri, M. N. (2021). A survey of data center consolidation in cloud computing systems. ComputerScience Review, 39, 100366.
21. Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 International Conference on Information Technology (ICIT) (pp. 779-786). IEEE.
22. Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET Communications, 14(7), 1185-1191.