CLOUD COMPUTING SECURITY ISSUES AND THEIR REMEDIES

Ms. Kshitija Patil, Ms. Minal Mandave, Faculty, Dept. of Computer Science Tilak Maharashtra Vidyapeeth, Pune-37

Abstract

The acceleration of cloud computing services has resulted in an increased pace of organisations outsourcing their computational services or monetizing their underutilised computational resources. Despite the allure of cloud migration from a financial standpoint, firms must consider many additional factors before making the decision to adopt this approach. One of the primary considerations pertains to security. While certain security concerns in cloud computing stem from the adopted solutions used to establish these services, numerous novel security inquiries specific to these solutions also emerge. These include questions regarding the organisation of services and the types of service/data that can be stored in the cloud. The present study aims to examine the many security concerns linked to cloud computing and put forward viable measures to alleviate these vulnerabilities. The research utilises a mixed-methods methodology, integrating an extensive examination of existing literature with a survey administered to experts in the field of information technology. This research emphasises the prevailing security concerns in cloud computing and offers significant insights into the proposed solutions and best practises as suggested by IT experts. The statement emphasises the relevance of adopting a comprehensive strategy to properly address these concerns and highlights the importance of ongoing monitoring and user education in upholding cloud security.

Keywords: Cloud Computing, Security issues, Remedies, Cloud Security

Introduction

In the context of cloud computing, the word "cloud" refers to a collection of interconnected networks. This analogy draws parallels to traditional clouds, which are composed of water molecules forming a pool of condensed vapour. According to the National Institute of Standards and Technology (NIST), cloud computing is a paradigm that enables the easy and on-demand access to a shared pool of customizable computing resources. These resources may include networks, servers, storage applications, and services. Cloud computing was developed by Amazon Web Services (AWS) and Microsoft Azure. These resources can be effortlessly controlled and used with very little effort on the part of the user or the cloud service provider [1]. The aforementioned system technique represents a cutting-edge information system that facilitates the dynamic sharing of resources over the Internet, hence yielding economic advantages.

Cloud computing has emerged as a result of the use and adaptation of virtual private networks (VPN) by service providers in data communication networks. There is a similarity between the virtualization situation seen in cloud computing, where resources are shared via the internet in a virtual environment. Cloud computing provides a range of services, including software, data calculation, storage services, and data access [2].

This technology does not prioritise the end-user's familiarity with the actual location, but rather emphasises the understanding of the system's setup that enables the provision of the service. The phrase in question represents a recent development in the field of computing that has rendered the traditional notion of physical, large-scale data centres obsolete. The relocation of physical storage, processing, and server facilities to third-party big data centres is facilitated [3]. Cloud computing has significantly transformed the distributed computing paradigm, enabling a highly flexible resource pool for storage and computational tasks. For some individuals, it serves as a means to use software and store data, while for others, it encompasses a package that provides a modified version of the distributed paradigm seen in cloud computing. It serves as a magnet for key societal components such as industry, academics, and enterprises, enabling them to minimise their collective expenditures on routine upkeep [4].

In the realm of information technology, this emerging paradigm of computing is making significant strides because to its advantageous features and its capacity to seamlessly adjust existing operational processes without hesitation [5]. The cloud model is subject to increased dangers and threats due to its significant prominence. The presence of vulnerabilities and loopholes in the security architecture of cloud computing services model serves as a catalyst for attracting attackers and hackers to engage in the pursuit of identifying and exploiting such weaknesses [6].

In recent years, a number of studies have been carried out with the purpose of conducting in-depth investigations into the issues of cloud computing's data security. It is essential to highlight the numerous open problems and vulnerabilities that need to be handled in the near future [7], as opposed to only concentrating on the benefits and advantages that are offered by the situation. This is necessary in order to enhance the trustworthiness and credibility of this technology, particularly in relation to its security parameters. The cloud computing concept presents many security concerns, including [8]:

- Safety precautions in cloud computing
- Vendor credibility assessment
- Risks associated with multi-tenancy in cloud computing
- Secure data management
- Evaluation of data portability levels

The system for maintaining Service Level Agreements (SLAs)

The following are a selection of unresolved scientific challenges pertaining to the cloud computing paradigm. The primary worry about the adoption of cloud computing is the pivotal role played by security factors from the user's viewpoint. This is due to the following reasons [9]:

The loss of control refers to the delegation of security management to a third-party entity, without the user's awareness of the specific place where the data is held and the security settings used to access this data [10].

The concept of multi-tenancy is a significant aspect in the field of computer science andThe concept of various tenants operating inside the same umbrella refers to the coexistence of several entities, either in terms of logical or physical medium. The service level agreement (SLA) should align the degree of expectation with the availability of access to stored data at all times [11].

The purpose of this research is to carry out an investigation into the many safety issues that are connected to the overall idea of cloud computing and to report our findings. The primary aim of this study is to provide a comprehensive analysis and categorization of the many attack vectors and security concerns associated with cloud computing technologies. Therefore, a comprehensive examination of the weaknesses and defects is conducted, with a focus on identifying their underlying causes. This study aims to enhance the knowledge and comprehension of cloud users, developers, providers, and other relevant stakeholders regarding the implementation and utilisation of cloud security concerns [12]. In order to ensure proactive and risk-free use of cloud computing, it is necessary to implement counterattack measures. To commence the discussion, it is imperative to provide an introductory overview of the architectural aspects pertaining to security concerns. Additionally, it is essential to highlight the significant implications and research problems associated with cloud security, as they play a crucial role in addressing security issues within the cloud computing paradigm [13].

CSA

The CSA is an entity that is overseen by a collective of professionals from various industries, firms, organisations, and other relevant parties, including notable companies such as Dell, HP, and eBay. One of the primary objectives of this initiative is to facilitate the widespread use of optimal methodologies for ensuring security in cloud computing systems [14].

This study examines three papers from the CSA, namely the security advice, the top dangers in cloud computing, and the Trusted Cloud Initiative (TCI) architecture. These documents include a significant portion of the ideas and guidelines that have been explored and disseminated by the CSA [15].

The most current edition of the CSA security advice, which is version 3.0, identifies multi-tenancy as one of the key characteristics of cloud computing. It is essential to keep in mind that the use of multi-tenancy particularly refers to the utilisation of shared resources by various consumers, perhaps belonging to different businesses or pursuing divergent goals [16]. Although virtualization is not required for the implementation of cloud infrastructures, it is essential to keep in mind that multi-tenancy specifically refers to the utilisation of shared resources.

The authors argue that, despite the potential resolution of virtualization-related problems, the implementation of segmentation and isolated regulations remains necessary for effective administration and protection of privacy.

The paper issued by CSA also addresses the identification of key hazards, with the intention of assisting in the development of risk management plans for the use of cloud solutions. The document focuses on challenges and difficulties that are particular to or exacerbated by core properties of cloud computing, such as shared infrastructures and more flexibility. The selection of cloud-specific challenges is noteworthy due to its potential to identify key areas for future advancement. In addition to this, the CSA security guidance is intricately connected to this collection of hazards, which helps to develop a solid foundation for carrying out security and risk analysis evaluations. In addition to this, it provides recommendations and ideas for best practises to achieve adequate levels of safety [17].

The Cloud Security Alliance (CSA) has implemented the TCI Reference Architecture Model as an additional strategy for structuring and managing cloud security and governance information. The primary objective of this paper is to delineate a set of principles that may facilitate the establishment of trust in cloud computing. Additionally, it aims to define open standards and capabilities that can be universally applied to all activities conducted in the cloud [18]. The design takes into account many different levels of organisation by including several frameworks and architectures, such as SABSA, TOGAF, ITIL, and Jericho. The SPI model, ISO 27002, COBIT, PCI, and SOX are some examples of the frameworks that have been integrated. Following that, a vast variety of contributing aspects will be discussed. The SABSA framework incorporates a number of different business operation support services, such as compliance, data governance, operational risk management, human resources security, security monitoring services, legal services, and internal investigations [19]. On the other hand, TOGAF outlines a number of distinct service categories, including presentation, application, information, and infrastructure services. ITIL is used for information technology operation and support, which includes IT operation, service delivery, support, and the management of incidents, modifications, and resources. ITIL was developed by the Information Technology Infrastructure Library. Last but not least, Jericho handles concerns pertaining to security and risk management. These concerns include information security management, authorisation, threat and vulnerability management, as well as rules and standards. The result is a three-dimensional connection between cloud delivery, trust, and operation, and the goal is for it to be easily utilised and deployed in a design that is centred on security [20].

Cloud Computing Security

There are many different security risks related with cloud computing, and prominent sources such as CSA's security guidelines and top threats analysis, ENISA's security evaluation, and NIST's cloud computing definitions give significant insights into these concerns. These concerns necessitate further research to effectively address them and thereby enhance the acceptance and adoption of cloud technology. The distinctions between software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS), which are generally used as the primary paradigm for classifying cloud services, are the focal point of this discussion. Nevertheless, there is a lack of standardisation and use of other techniques for organising the security components of cloud computing, outside from the categorization of cloud deployment strategies, service kinds, and conventional security models [21].

This part attempts to identify the key issues in this subject and organise them into a model consisting of seven categories, relying upon the sources that were previously stated in order to accomplish the goals of focussing and organising content relevant to cloud security and making it easier to conduct future research. In addition, this section will facilitate future study. This research looks specifically at network security, interfaces, data security, virtualization, governance, compliance, and legal problems [22]. The specific topics that are covered include these and more.

It is possible to draw the conclusion that cloud security encompasses both traditional and well-known challenges, such as vulnerabilities in network and infrastructure, user access, authentication, and privacy, as well as emerging concerns arising from the adoption of new technologies to provide appropriate resources, primarily virtualized ones, services, and auxiliary tools [23]. This conclusion can be reached on the basis of the pointss that have been discussed so far.

The problems that need to be solved may be broken down into many categories, including data location and e-discovery, hypervisor vulnerabilities, data isolation, and a loss of control over data, security, and decision making. These concerns have been identified as the primary technical, legal, and strategic considerations, respectively, based on the studies and graphics presented [24].

In conclusion, an examination of contemporary patterns in cloud computing indicates the existence of a significant array of well researched security issues. These concerns have been addressed via the development of several solutions and the establishment of best practises, particularly in relation to legal and administrative matters. However, it is important to note that there are still several unresolved problems that need more research endeavours, particularly in the realm of safe virtualization.

Methodology

- A complete assessment of articles, books, reports, and whitepapers that were subjected to peer review and were connected to cloud computing security problems was carried out for this section of the study. Data security, network security, and access control were determined to be the three most important categories for organising security concerns. On the basis of the literature research, solutions and recommendations for best practises were found.
- Design of the Survey: In order to collect information on the experiences and perspectives of IT professionals with respect to the safety of cloud computing, a structured questionnaire was developed. In the survey, we included questions about the respondents' experiences with various security issues, as well as the solutions that they had personally developed or would propose to others.
- Distribution of the Survey: The survey was circulated to IT professionals working in a variety of businesses by using internet platforms, professional networks, and email invites to distribute the survey. Over the course of one and a half quarters, a total of two hundred fifty replies were gathered.
- Analysis of the Data: Statistical software was used to conduct an analysis of the quantitative data gathered from the survey. The replies that were given in qualitative format were sorted into categories and subjected to a theme analysis in order to determine recurrent problems with security and possible solutions.

Results

1) Concerns Regarding the Safety of Cloud Computing:

a) Problems with Data Security:

- Sixty-two percent of respondents said that their organisation has experienced data breaches or unauthorised access.
- Concerns regarding the possible loss of data during relocation were voiced by 48% of respondents.

b) Concerns Regarding Network Security:

- Fifty-four percent of respondents voiced their worries about potential network vulnerabilities and DDoS assaults.
- 37 percent of respondents reported having trouble monitoring and protecting data flows over the internet.

c) Concerns Regarding Access Control:

- Forty-nine percent of respondents voiced their worries about insufficient access control systems.
- Having difficulty successfully managing user rights and responsibilities was stated by 43% of respondents.

Table 1: Security Issues in Cloud Computing

Security Issues	**Percentage of Respondents**
Data Security Issues	
- Data breaches	62%
- Unauthorized access	62%
- Data loss during migration	48%
Network Security Issues	
- Network vulnerabilities	54%
- DDoS attacks	54%
- Monitoring data transit	37%
Access Control Issues	
- Inadequate access control	49%
- User permission management	43%

2) Treatments and Recommended Procedures:

a) Data Security Measures:

- Encryption both while the data is at rest and when it is being transferred (recommended by 68% of respondents).
- Data backups and disaster recovery strategies that are updated on a regular basis (recommended by 55% of respondents).

b) Network Security Remedies:

- The installation of an effective firewall and intrusion detection system (suggested by 61% of respondents).
- Ongoing monitoring and danger detection in real time (suggested by 48 percent of respondents).

c) Access Control Solutions:

- Implementation of Multi-Factor Authentication (MFA) (63% of respondents preferred this solution).
- Conducting access audits and privilege assessments on a regular basis (52% of respondents suggest this).

Table 2: Remedies and best practices

Remedies and Best Practices	**Percentage of Respondents Recommending**
Data Security Remedies	
- Encryption at rest and in transit	68%
- Regular data backups and disaster recovery plans	55%
Network Security Remedies	
- Implementation of robust firewall and intrusion detection systems	61%
- Continuous monitoring and real-time threat detection	48%
Access Control Remedies	
- Implementation of multi-factor authentication (MFA)	63%
- Regular access audits and privilege reviews	52%

3) Recurring Themes in Qualitative Responses:

- A significant number of interviewees emphasised the need of implementing staff training and awareness programmes in order to improve safety.
- Providers of cloud services were strongly urged to make their security documentation and compliance reports public and transparent.

Conclusion

The quickening speed of cloud computing services has led to a rise in the number of businesses either outsourcing their computational services or monetizing their computational resources that are going unused. Before deciding whether or not to follow this strategy, businesses need to give careful consideration to a great deal of extra information, despite the fact that cloud migration is financially appealing. The problem of ensuring everyone's safety is without a doubt one of the most significant considerations. There are a number of new security concerns that develop as a result of the usage of these existing solutions to set up the cloud computing services; however, there are also a number of security concerns that are produced by the cloud computing solutions themselves. These issues include questions about the configuration of services as well as the types of data and services that may be stored in the cloud. Additionally, there are questions regarding the types of data and services that may be preserved in the cloud. The purpose of this research is to investigate the myriad of security issues that are associated with cloud computing and to provide workable solutions to the problems that have been identified. The investigation makes use of an approach known as mixed methods, which combines an in-depth review of the previously published material with a survey that is given to knowledgeable individuals working in the area of information technology. This study highlights the prevalent security risks in cloud computing and provides key insights into the recommended remedies and best practises as indicated by IT professionals. The research also highlights the importance of cloud computing to the future of computing. The statement underlines the necessity of establishing a complete plan to effectively handle these problems and underscores the need of continual monitoring and user education in sustaining cloud security. Additionally, the statement highlights the importance of addressing these concerns in a timely manner.

References

[1]Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., &Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*, 1-18.

[2]Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, *75*, 200-222.

[3]Modi, C., Patel, D., Borisaniya, B., Patel, A., &Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing*, *63*, 561-592.

[4]Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications*, *7*(4).

[5]Batra, M., & Gupta, N. (2016). Various security issues and their remedies in cloud computing. *Int. J. Adv. Eng. Manag. Sci.(IJAEMS)*, *2*(2), 18-20.

[6]Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *2012 international conference on computer science and electronics engineering* (Vol. 1, pp. 647-651). IEEE.

[7]Saxena, R., &Gayathri, E. (2021, October). A study on vulnerable risks in security of cloud computing and proposal of its remedies. In *Journal of Physics: Conference Series* (Vol. 2040, No. 1, p. 012008). IOP Publishing.

[8]Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of internet services and applications*, *4*, 1-13.

[9]Aich, A., Sen, A., & Dash, S. R. (2015, January). A survey on cloud environment security risk and remedy. In *2015 International Conference on Computational Intelligence and Networks* (pp. 192-193). IEEE.

[10]Dillon, T., Wu, C., & Chang, E. (2010, April). Cloud computing: issues and challenges. In *2010 24th IEEE international conference on advanced information networking and applications* (pp. 27-33). Ieee.

[11]Liu, Y., Sun, Y. L., Ryoo, J., &Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: solutions and future directions.

[12]Hussain, I., & Ashraf, I. (2014). Security issues in cloud computing-a review. *International Journal of Advanced Networking and Applications*, *6*(2), 2240.

[13]Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., &Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, *51*, 2172-2175.

[14]Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

[15]Ali, M., Khan, S. U., &Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.

[16]Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet computing*, *16*(1), 69-73.

[17]Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., &Albaqami, N. (2023). Cloud security threats and solutions: A survey. *Wireless Personal Communications*, *128*(1), 387-413.

[18]Yenugula, M., Sahoo, S., &Goswami, S. (2023). Cloud computing in supply chain management: Exploring the relationship. *Management Science Letters*, *13*(3), 193-210.

[19]Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

[20]Agapito, G., &Cannataro, M. (2023). An Overview on the Challenges and Limitations Using Cloud Computing in Healthcare Corporations. *Big Data and Cognitive Computing*, *7*(2), 68.

[21]Shrinivasa, D. C. B. (2023). A Review on Chronicle of Cloud Computing Security and Storage Environment Models. *Journal of Survey in Fisheries Sciences*, *10*(3S), 1112-1125.

[22]Tsochev, G. R., &Trifonov, R. I. (2022). Cloud computing security requirements: A Review. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1216, No. 1, p. 012001). IOP Publishing.

[23]Sasubilli, M. K., &Venkateswarlu, R. (2021, January). Cloud computing security challenges, threats and vulnerabilities. In *2021 6th international conference on inventive computation technologies (ICICT)* (pp. 476-480). IEEE.

[24]Balani, Z., &Varol, H. (2020, June). Cloud computing security challenges and threats. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-4). IEEE.