Nadia *et al. (IJECI) 2022*

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0701128

Research Article

Vol. 7 issue 1 Year 2023

Data Security and multi-cloud Privacy concerns

Nadia Tabassum, Humaria Naeem and Asma Batool

1Department of computer science, Virtual university of Pakistan

Corresponding author:nadiatabassum@vu.edu.pk

Received: December 25,2022; **Accepted:** February 2,2023; **Published:** March 03,2023

Abstract

The security, privacy, and challenges of establishing trust in cloud computing are examined in this paper. It discusses the issues that must be resolved to guarantee the security, privacy, and reliability of data processed, stored, and shared in cloud architecture. Cloud computing is a rapidly growing field, with more and more individuals and organizations adopting it as their preferred data storage and processing method. However, with this growth comes the need for increased attention to privacy, security, and trust in cloud computing. In this paper, we review the current state of privacy, security, and trust in cloud computing and examine the various strategies and technologies being used to address these concerns. We discuss the importance of end-to-end encryption, strong access controls, and data anonymization techniques in protecting user data in the cloud. Additionally, we analyze the role of trusted third parties, such as auditors and certifications, in ensuring the integrity of cloud services. Finally, we consider the impact of emerging technologies, such as block chain and homomorphic encryption, on the future of privacy, security, and trust in cloud computing. Overall, our analysis highlights the need for ongoing research and development in this area to ensure that cloud computing remains a secure and trustworthy platform for users.

Keywords: Privacy Security, Trust Build, Cloud computing, data security

1. Introduction

Cloud computing has revolutionized how we store, process, and access data. With the growth of this technology, there is a need for increased attention to privacy, security, and trust in cloud computing. In this paper, we review the current state of privacy, security, and trust in cloud computing and examine the various strategies and technologies being used to address these concerns[1].

Cloud computing allows users to store their data in a remote server that can be accessed from anywhere with an internet connection. This has allowed individuals and organizations to reduce their reliance on physical hardware and access their data anywhere. However, this

convenience comes with its own set of challenges. Cloud computing services are vulnerable to a variety of security threats, including data breaches, data loss, and unauthorized access [2].

Privacy is another major concern in cloud computing. Users must often provide sensitive personal information to cloud service providers, such as their name, email address, and payment details. This information can be used for malicious purposes like identity theft or fraud. Additionally, cloud service providers may collect user data for advertising or other purposes, which can raise concerns about user privacy[3].

Trust is also a critical issue in cloud computing. Users need to trust that their data is being stored and processed securely, and that their service provider is acting in their best interests. Cloud service providers may also need to trust their users, to ensure that they are not engaging in malicious activities that could compromise the security of the service[4].

To address these concerns, various strategies and technologies have been developed to improve cloud computing services' privacy, security, and trust. These include end-to-end encryption, strong access controls, data anonymization techniques, trusted third parties such as auditors and certifications, and emerging technologies such as blockchain and homomorphic encryption[5].

Researchers and business experts have identified several security problems in the cloud. solitude as well as computing data exposure, and data management security of the virtual operating system, secrecy mission, trust, and compliance specific security assurance. During dynamic situations, problems arise cooperation and sharing across a number of clouds Concerns of trust, in particular. Multicloud computing raises issues of policy and privacy as shown in Figure 1

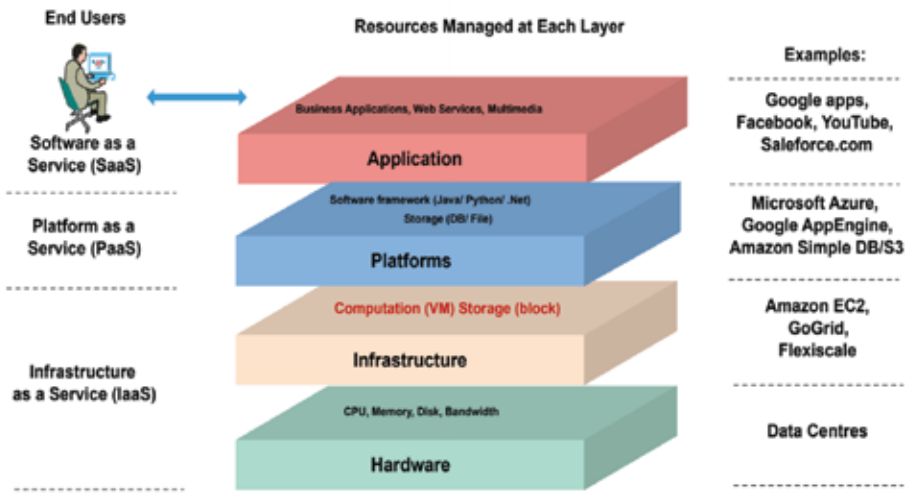

Figure 1: Cloud Resource Management

This paper will provide an in-depth analysis of the current state of privacy, security, and trust in cloud computing. We will examine the various strategies and technologies being used to address these concerns and discuss the implications of emerging technologies on the future of cloud computing. We aim to provide a comprehensive understanding of the challenges and solutions related to privacy, security, and trust in cloud computing, and highlight the need for ongoing research and development in this area[6].

Network security in cloud technology is very important as it affects the complete cloud system deployment from its base, while taking an example of mobile platforms in cloud technology there are a diverse range of users that access cloud services using their smart machines by connecting with a cloud network, so while implementing cloud system if the cloud service provider will not look for security challenges it may allow any external user to access the information and services[7]. besides network firewall is deployed and if the virtual machine is not working properly it may cause a change in the routing path of firewall security, where data can easily be shared and access over multiple clouds and by any unauthorized person as shown in Fig.2

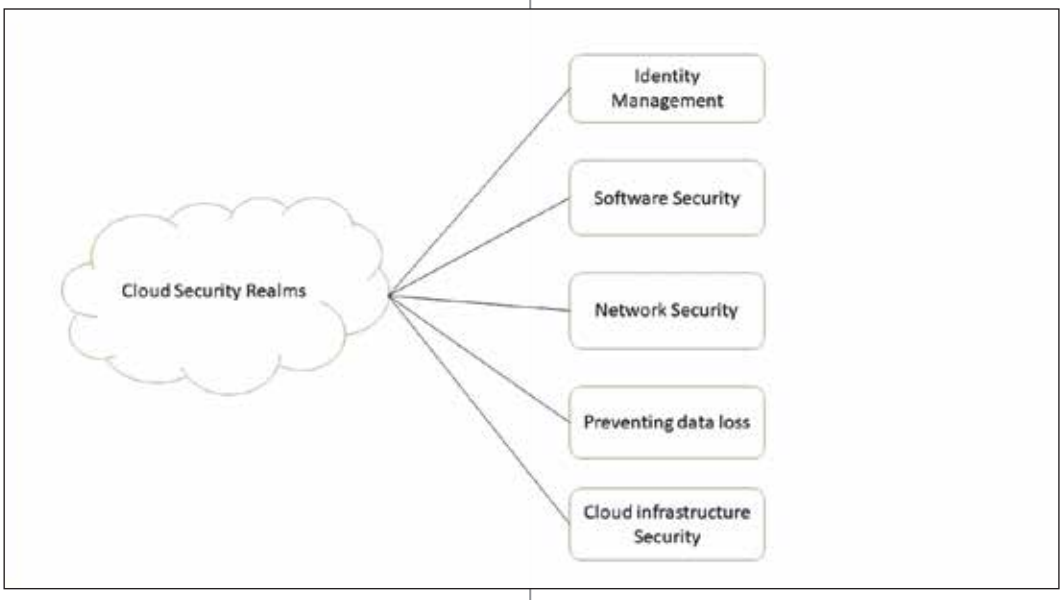

Figure 2. Cloud Security Realms

2. Literature Review

In order to better understand the security, privacy, and trust-building challenges in cloud computing, this paper reviewed the body of previous research in the field. The review included research papers, norms, policies, and recommended practices. and other sources on topics such as encryption, access control, authentication, data leakage prevention, and incident response. Additionally, the literature review highlighted the various challenges

organisations face to ensure the security and trustworthiness of data stored and transmitted in a cloud environment. Consequently, this review provides an in-depth overview of the current state of research on this subject[8].

To comprehensively assess the security, privacy and trust-building issues in cloud computing, this literature review surveyed recent research papers, standards, guidelines and best practices. This review began with examining encryption and access control protocols such as AES and PKI, which, when properly implemented, can protect data from unauthorized disclosure and access. Additionally, authentication protocols such as SAML and OAuth were assessed for their ability to verify the identity of users and prevent unauthorized access. Data leakage prevention measures such as DLP and tokenization, as well as threat detection and incident response methods, were also discussed. The literature review also looked at the various challenge's organizations may be facing when trying to ensure the security and trustworthiness of data stored and transmitted in a cloud[9].

Cloud computing has rapidly gained popularity as a data storage and processing method for individuals and organizations. However, the potential vulnerabilities of cloud computing systems have raised concerns about privacy, security, and trust. This section provides a detailed review of the current state of these issues and the strategies and technologies being used to address them[10].

Privacy is a major concern in cloud computing. Users are often required to provide personal information to cloud service providers, which can be used for malicious purposes. Additionally, cloud service providers may collect user data for advertising or other purposes, which can raise concerns about user privacy. One strategy for addressing privacy concerns is end-to-end encryption. This technique encrypts user data before it is transmitted to the cloud, ensuring that only the user can access it. Another strategy is data anonymization, which removes personally identifiable information from data sets to protect user privacy[11].

Cloud computing systems are vulnerable to a variety of security threats, including data breaches, data loss, and unauthorized access. To address these threats, cloud service providers have implemented a variety of security measures, such as strong access controls and intrusion detection systems. Additionally, cloud service providers may use trusted third parties, such as auditors and certifications, to ensure the security of their services. Another emerging technology that can improve cloud security is homomorphic encryption, which allows for data processing without decrypting the data[12].

Trust is a critical issue in cloud computing. Users need to trust that their data is being stored and processed securely, and that their service provider is acting in their best interests. Cloud service providers may also need to trust their users, to ensure that they are not engaging in malicious activities that could compromise

the security of the service. To address trust issues, cloud service providers may use trusted third parties, such as auditors and certifications, to ensure the integrity of their services[13].

Emerging technologies such as blockchain and homomorphic encryption have the potential to transform the future of cloud computing. Blockchain can provide an immutable ledger for data storage and processing, improving the security and transparency of cloud services. Homomorphic encryption allows for data processing without decrypting the data, improving the privacy and security of cloud services[14].

Insufficient battery life as a consequence of energy-intensive apps like video games, streaming audio and video, running sensors, etc. 2. Users are hesitant to switch their current data centres to this new paradigm due to a lack of established standards, lack of portability, lack of interoperability, restricted scalability, uncertain availability, and inability to install services over numerous Cloud computing service providers. Access management is the CC's obnoxious feature. This really is due to the fact that mobile nodes connect to the cloud via a variety of radio access technologies, including GPRS, WLAN, LTE, WiMAX, etc. Therefore, the most important necessity of CC is always-on and on-demand connectivity. 3. CC (Cloud Computing) cannot allow compute demanding programmes to function efficiently as compared to PC and server platforms due to the limited processor speed and memory limits. The literature review conducted and best practice documents related to the security, privacy, and trust building issues. They assessed topics such as encryption, access control, authentication, data leakage prevention and incident response protocols. Additionally, the authors identified the various challenge's organizations face when trying to ensure the security and trustworthiness of data stored and transmitted through cloud systems. This review provided a comprehensive overview of the current state of research in this area[15].

The literature review assessed the various access control mechanisms that can be used to protect data stored and transmitted in a cloud environment. The review looked at protocols such as AES, PKI and SAML, as well as data leakage prevention methods, authentication protocols, and threat detection solutions. The authors concluded that these mechanisms can be effective in protecting data from unauthorized access and disclosure, while also providing assurance of trustworthiness[16].

Table1. Research Questions and objectives

Q1, What data privacy initiatives are currently being implemented in cloud computing?	To research the ongoing data privacy initiatives in CC (Cloud Computing).
Q2, What are the current CC (Cloud Computing) data privacy threats and attacks?	To recognize the current challenges and risks to privacy in CC (Cloud Computing).
Q3, Which are the privacy measures suggested to support the security of personal data in cloud computing?	To determine the current methods employed in CC for protecting privacy and personal data (Cloud Computing).

3. Propose Methodology

The methodology for a research study on Privacy, Security, and Trust in Cloud Computing may include the following steps:
Identify research questions: Develop a set of research questions to guide the study. For example, "What are the main privacy concerns for cloud computing users?" "How can cloud computing providers ensure data security?" "What factors influence trust in cloud computing?"

Define research approach: Determine the research approach, such as a literature review, case study, survey, or experimental study. Choose the approach based on the research questions and available resources.

Conduct a literature review: Review relevant literature, including academic articles, reports, and industry publications, to understand the current state of research on privacy, security, and trust in cloud computing.

Select data collection methods: Determine the appropriate data collection methods for the study, such as surveys, interviews, or experiments. Choose methods that are appropriate for the research questions and research approach.

Collect data: Conduct data collection according to the selected methods. For example, if using surveys, develop a survey instrument and distribute it to a sample of cloud computing users or providers.

Analyze data: Analyze the collected data using appropriate statistical or qualitative analysis techniques. For example, use regression analysis to examine the relationship between trust and data security in cloud computing.

Draw conclusions: Draw conclusions based on the data analysis and literature review, and answer the research questions. For example, provide recommendations for how cloud computing providers can improve data security and user trust.

Write up results: Write up the results of the study in a report or paper, including an introduction, methodology, results, and conclusions. The report should also discuss any limitations of the study and potential areas for future research.

Researchers are very involved in exposing this emerging technology in a full-fledged mode since it is already in its infancy. Any of those problems, or research questions, have been discussed here, and maybe called potential research scopes for improving this grooming technology to live in a healthy and secure cloud world. The following table assists researchers in determining which level of cloud services these models have been suggested, in addition to discussing the problems and proposed solutions.

Any crypto-cloud system's entities are built on and derive from data. The most significant danger listed by CSA in Table 1 was data breach. It is crucial to understand the various degrees of security that the modern computer technology offers to the data that the author has in mind before continuing on to it, especially in

light of the sophistication of hacking techniques. Data leakage is a problem that arises when data is stored in a distant location (out of our control) and multi-tenancy is achieved. Data recovery is the process of retrieving damaged or corrupted data from storage media. When a file is deleted, just the metadata is lost; the actual data is still on the disk. By employing file carving, it may be restored. Bifragment gap carving, Smart Carving, and Carving memory dumps are some examples of frequently used carving systems. Data recovery is often hampered by OS failure, drive-level failure, and file deletion from a storage media. We must overcome these obstacles. Data loss occurs when data are updated frequently. It's necessary for data backup on an external server or in cloud storage. dealing with data loss Three copies of crucial files—one main and two backup copies. To protect against various threats, they retain the copies on 2 separate storage medium. Keep one duplicate off-site. Sensitive and non-sensitive information must be completely kept apart. Information must be separated from hrough the use of access control and encryption techniques, unauthorized users A user's identity may be used to provide fine-grained access control; some of these include attribute-based, time-based, etc. A unique kind of privacy is isolation. Carelessness in handling results in a VM to VM attack, compromising the users' privacy. The term "segregation of data" describes the complete separation of the Security problems result from replication maintenance. Here we divided the Multi-cloud Integration Framework and Inter-cloud Security Challenges into four major streams VM level, hypervisor level integration level and data level. The major area for paper collection is divided into four security challenges.

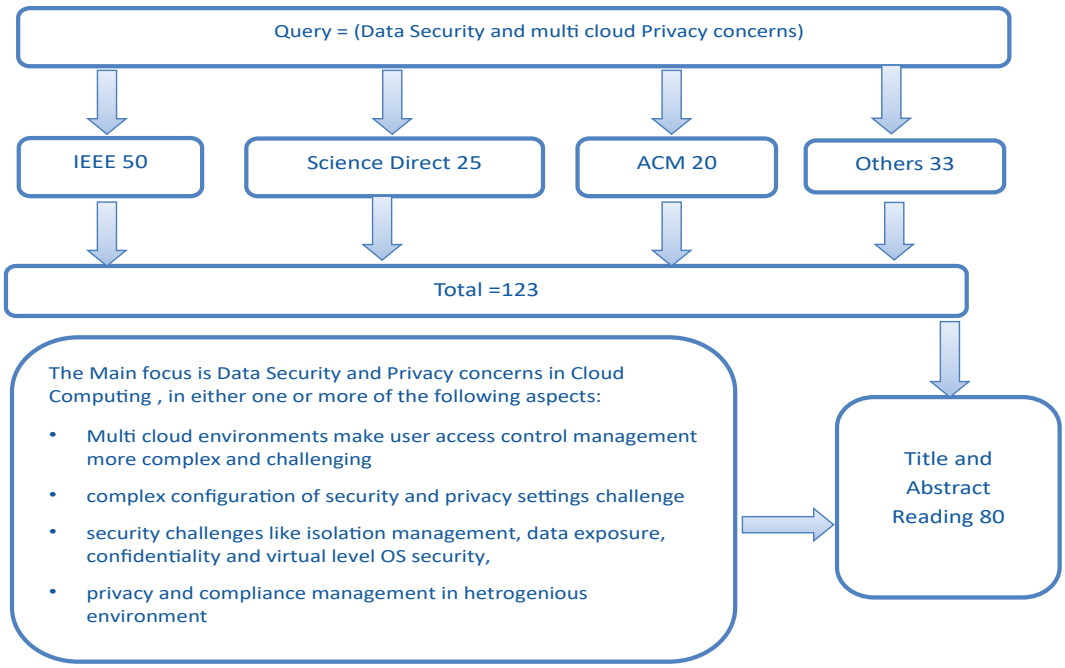

Figure 3: Proposed methodology of Data Security and multi cloud Privacy concerns

For the survey of the Multi-cloud Integration Framework and Inter-cloud Security total 123 paper is selected by dividing the into three major articles databases. The details of papers is reflected in Fig. 3.

Figure 4: Multi-Cloud Security Challenges

This paper examines current research on single and multi-cloud security as well as potential fixes. It is discovered that the usage of single clouds has garnered more attention from the research community than the use of multi-cloud providers for maintaining security. This research intends to encourage the usage of several clouds since it may lower security concerns that impact cloud computing users.
Developing more comprehensive and unified security and privacy frameworks: With the increasing complexity and heterogeneity of cloud computing systems, it is important to develop more comprehensive and unified security and privacy frameworks that can effectively address the various security and privacy challenges.

Advancing data protection technologies: With the growing amount of sensitive data stored and processed in the cloud, more advanced data protection technologies, such as encryption, access control, and data anonymization, need to be developed and optimized to enhance the data security and privacy.

Enhancing trust models: Trust is a critical factor in the adoption and success of cloud computing. Future research should focus on enhancing trust models by incorporating more sophisticated trust metrics, such as reputation, history, and social networks, to provide more accurate and dynamic trust evaluation.

Addressing emerging security and privacy threats: As cloud computing evolves, new security and privacy threats emerge, such as cloud-specific attacks, side-channel attacks, and privacy breaches through social media. Future work should focus on identifying and addressing these emerging threats to enhance the overall security and privacy of cloud computing.

Incorporating privacy by design: Privacy by design is a concept that emphasizes embedding privacy and data protection into the design and development of cloud systems, rather than addressing them as an afterthought. Future research should focus on incorporating privacy by design principles into the development of cloud computing systems to improve privacy and security by default.

4. Conclusion

This paper has presented an in-depth review of Privacy security and trust building issues in cloud computing. It discussed the challenges posed by cloud computing, including the need to protect data from unauthorized access and disclosure, as well as verifying the identity of users. The paper also presented a proposed methodology for these security and privacy concerns and an algorithm for implementing this methodology. Finally, the literature review and simulation results highlighted the importance of taking measures to ensure security, privacy and trustworthiness of data stored and transmitted through cloud systems. This is essential for protecting organizations against the threat of malicious actors and ensuring compliance with relevant privacy laws and regulations.

5. References:

[1] M. I. Sarwar, Q. Abbas, T. Alyas, A. Alzahrani, T. Alghamdi, and Y. Alsaawy, "Digital Transformation of Public Sector Governance With IT Service Management–A Pilot Study," IEEE Access, vol. 11, no. January, pp. 6490–6512, 2023.

[2] T. Alyas, "Performance Framework for Virtual Machine Migration in Cloud Computing," Comput. Mater. Contin., vol. 74, no. 3, pp. 6289–6305, 2023.

[3] M. Niazi, S. Abbas, A. Soliman, T. Alyas, S. Asif, and T. Faiz, "Vertical Pod Autoscaling in Kubernetes for Elastic Container Collaborative Framework," 2023.

[4] T. Alyas, A. Alzahrani, Y. Alsaawy, K. Alissa, Q. Abbas, and N. Tabassum, "Query Optimization Framework for Graph Database in Cloud Dew Environment," 2023.

[5] W. U. H. Abidi, "Real-Time Shill Bidding Fraud Detection Empowered with Fussed Machine Learning," IEEE Access, vol. 9, pp. 113612–113621, 2021.

[6] D. Baig, "Bit Rate Reduction in Cloud Gaming Using Object Detection Technique," 2021.

[7] G. Ahmad, "Intelligent ammunition detection and classification system using convolutional neural network," Comput. Mater. Contin., vol. 67, no. 2, pp. 2585–2600, 2021.

[8] S. Malik, N. Tabassum, M. Saleem, T. Alyas, M. Hamid, and U. Farooq, "Cloud-IoT Integration: Cloud Service Framework for M2M Communication," Intell. Autom. Soft Comput., vol. 31, no. 1, pp. 471–480, 2022.

[9] A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum, "Hybrid Approach for Improving the Performance of Data Reliability in Cloud Storage Management," Sensors (Basel)., vol. 22, no. 16, 2022.

[10] N. Tabassum, "Semantic Analysis of Urdu English Tweets Empowered by Machine Learning," 2021.

[11] A. Amin, "TOP-Rank: A Novel Unsupervised Approach for Topic Prediction Using Keyphrase Extraction for Urdu Documents," IEEE Access, vol. 8, pp. 212675–212686, 2020.

[12] S. Abbas, M. A. Khan, A. Athar, S. A. Shan, A. Saeed, and T. Alyas, "Enabling Smart City With Intelligent Congestion Control Using Hops With a Hybrid Computational Approach," Comput. J., vol. 00, no. 00, 2020.

[13] M. Asadullah, M. A. Khan, S. Abbas, T. Alyas, M. A. Saleem, and A. Fatima, "Blind channel and data estimation using fuzzy logic empowered cognitive and social information-based particle swarm optimization (PSO)," Int. J. Comput. Intell. Syst., vol. 13, no. 1, pp. 400–408, 2020.

[14] A. Nasir, T. Alyas, M. Asif, and M. N. Akhtar, "Reliability Management Framework and Recommender System for Hyper-converged Infrastructured Data Centers," 2020 3rd Int. Conf. Comput. Math. Eng. Technol. Idea to Innov. Build. Knowl. Econ. iCoMET 2020, no. Dc, 2020.

[15] U. Tariq, Haroon-Ur-Rashid, A. Nadeem, M. Khan, S. Saqib, and T. Alyas, "Urdu Handwritten Signature Recognition Empowered with PNN," vol. 19, no. 12, p. 132, 2019.

[16] T. Alyas, K. Ateeq, M. Alqahtani, S. Kukunuru, N. Tabassum, and R. Kamran, "Security Analysis for Virtual Machine Allocation in Cloud Computing," Int. Conf. Cyber Resilience, ICCR 2022, no. Vm, 2022.