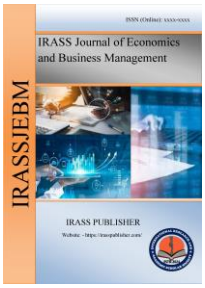
IRASS Journal of Economics and Business Management
Abbriviate Title- IRASS J Econ Bus Manag
ISSN *(Online) 3049-1320*
https://irasspublisher.com/journal-details/IRASSJEBM
Vol-1, Iss-1(December-2024)



Understanding Information Security on Cloud Computing

Firzah Hafiz Deandra[1*], Sherly[2], Iskandar Muda[3], Gusnardi[4]

[*1-2-3]Universitas Sumatera Utara, Medan, Indonesia

[4] Universitas Riau, Pekanbaru, Indonesia

Corresponding Author Firzah Hafiz Deandra

School of Sceince and Tehmology Federal Polytechnic Kaura Namoda Zamfara State.

Article History

Received: 22 / 11/ 2024

Accepted: 10 / 11 / 2024

Published: 14 / 12 / 2024

Abstract: As cloud computing becomes increasingly prevalent, ensuring robust information security is essential to protect sensitive data from evolving cyber threats, especially in shared cloud infrastructures where unique vulnerabilities arise. This study aims to explore the impact of information security on cloud computing through a systematic literature review of articles sourced from reputable databases such as Science Direct, Emerald Insight, MDPI, and Taylor & Francis. The findings highlight that cloud security is anchored in securing systems, infrastructure, user authentication, and networks. Advanced techniques like the Attack Defense Model, Graph Neural Networks, and Homomorphic Encryption are used to address threats, while user behavior and strong architectural designs are critical factors. Continuous evaluation and anomaly detection further enhance security in cloud environments. This research contributes to understanding the relationship between information security and cloud computing, offering practical strategies for organizations and cloud service providers to mitigate risks, build trust, and ensure data protection in the cloud.

Keywords: Cloud computing, data protection, cloud environment, impact of information security, cyber threats.

1. Introduction

1.1 Background

Information security has become a cornerstone of modern digital operations, as the protection of sensitive data and the assurance of confidentiality, integrity, and availability are critical for organizations across industries. As cyber threats continue to evolve in both complexity and frequency, ensuring robust security measures has become a top priority for businesses and individuals alike. Failures in information security can lead to severe consequences, including data breaches, financial loss, reputational damage, and legal repercussions [11]. Consequently, organizations are investing heavily in security strategies, technologies, and practices to protect their information systems from threats and vulnerabilities.

In parallel with these security concerns, cloud computing has gained immense popularity due to its ability to provide scalable, cost-efficient, and accessible computing resources. However, as organizations increasingly migrate their critical operations and sensitive data to the cloud, the intersection between information security and cloud computing has become a major area of concern. Cloud environments, while offering numerous benefits, also introduce unique security risks such as data breaches, unauthorized access, and vulnerabilities in shared infrastructures. As digital technologies advance, information security has become a critical concern across all industries. Cloud computing, while offering numerous advantages such as scalability and cost efficiency, introduces new security risks that can expose sensitive data to potential threats [12]. Issues like data breaches, unauthorized access, and vulnerabilities in shared systems raise concerns about the safety of information stored in the cloud. These risks make it difficult for organizations to fully trust cloud services, as a security failure could lead to significant financial, legal, and reputational damage.

The primary objective of this research is to examine the impact of information security on cloud computing. This involves identifying key security risks associated with cloud environments, such as data breaches, unauthorized access, and vulnerabilities in shared infrastructure, and understanding how these risks affect organizations. Additionally, the research will analyze the security measures implemented by cloud service providers (CSPs) to mitigate these risks, including encryption, access controls, and threat detection systems. Another objective is to assess how organizational policies and industry standards shape security requirements for cloud computing and influence companies' decisions to adopt these services. The research will also evaluate user perceptions and trust in cloud computing services.

1.2 Benefit of Research

1.2.1 Theoretical Benefit

The theoretical benefits of this research contribute to the existing body of knowledge in several ways. First, it will enhance the understanding of the relationship between information security and cloud computing, providing a framework for analyzing how security risks influence the adoption and effectiveness of cloud services. This

research will fill gaps in the literature by exploring the specific security challenges organizations face when migrating to the cloud and how these challenges can deter or enable cloud adoption. Additionally, it will contribute to the development of theories related to trust in technology, highlighting the factors that affect user confidence in cloud services. By examining the role of security measures in fostering trust, the research may also lead to new theoretical insights into the dynamics of risk management in cloud computing environments.

1.2.2 Practical Benefit

The research offers valuable insights and recommendations for organizations and cloud service providers. For organizations contemplating the transition to cloud computing, the findings will provide a clear understanding of the security risks involved and actionable strategies for mitigating these risks, enabling informed decision-making. The study will evaluate the effectiveness of various security measures employed by cloud service providers, guiding organizations in selecting reliable and secure cloud solutions. Additionally, the research will address user perceptions and trust issues, helping cloud providers better understand their clients' concerns and improve their service offerings. The practical recommendations generated from this study will serve as a resource for organizations looking to enhance their data security practices in cloud environments, ultimately leading to improved data protection, compliance with relevant regulations, and a reduction in the risk of data breaches. Furthermore, by exploring emerging threats to cloud security.

2. Literature Review

2.1 Information Security

Information security is defined as the activity to protect information from a wide range of threats in order to ensure business continuity, minimize business damage, and maximize return on investments and business opportunities (Hagen, Albrechsten, & Hovden, 2008) In today's organizations, information is a crucial asset. Without reliable and securely managed information, businesses are likely to face significant challenges or even fail. Surprisingly, despite the numerous advantages that come from investing in security such as protecting valuable information assets and avoiding serious repercussions many organizations still underinvest in security measures. Chief security officers often note that demonstrating the value of security investments can be challenging unless a disaster occurs.

The management of information directly impacts an organization’s reputation. Maintaining a sufficient level of security is a vital component of effective information and information systems management. Security should be integrated into system design to align with the existing security framework. This security architecture is not merely a collection of products but rather a structured model that outlines essential services, including authentication, authorization, auditing, and intrusion detection, that must be supported by technology. It provides a benchmark for evaluating applications. Additionally, security architecture helps developers understand that various applications require similar security services and should be built according to a unified security model.

2.2 Cloud Computing

Cloud computing is the delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the internet to offer faster innovation, flexible resources, and economies of scale [13]. Cloud computing is a term used to describe the on-demand delivery of computing resources, namely hardware, storage, databases, networks, and software, to businesses and individuals over a network. With cloud computing, organizations can access and store information without the need to manage their own physical devices or IT infrastructure.

Cloud computing offers several advantages for businesses, including faster product deployment, scalability, cost savings, improved collaboration, and enhanced security. Users can quickly launch or stop new instances within seconds, allowing developers to accelerate their work and test new ideas without being limited by hardware or slow procurement processes. Additionally, cloud computing provides flexibility, enabling businesses to rapidly scale their resources and storage to meet demand without needing to invest in physical infrastructure. Companies only pay for the resources they actually use, avoiding the costs associated with building and maintaining excessive data centers, while also freeing up valuable IT team time for more strategic initiatives. Furthermore, cloud storage ensures data is accessible anytime and anywhere, allowing people to work from any location with an internet connection. Contrary to common perceptions, cloud computing can actually enhance security due to its advanced security features, automated maintenance, and centralized management. Leading cloud providers hire top security experts and utilize cutting-edge solutions, offering stronger protection. They also provide backup and disaster recovery features, helping to prevent data loss in emergencies, such as hardware failures, security threats, or even user errors.

3. Methods

In line with the stated objectives, this research provides answers to the following questions, namely (1) What is the research context used for Information Security used on Cloud Computing (2) What is the method used for the adoption of Information Security (3) What factors influence Information Security on Cloud Computing.

3.1 Search Process

To select relevant literature, published articles on Information Security and Cloud Computing were collected worldwide and drawn from reputable literature databases such as Science Direct, Emerald Insight, MDPI, Taylor & Francis and another journals uses information security or cloud computing as a subject.The keywords used in the search were "Information Security", "IS", "Cloud Computing", "Cloud Data Protection" and "Cloud Security Risk". The following is a screening based on the inclusion and exclusion criteria listed in Table 1.

Table 1. Inclusion and exclusion criteria

Inclusion Criteria	Exclusion Criteria
• Publish in 2017-2024 • Journal related to Information Security and Cloud Computing	• Journals that are not in English • *PDF Not Available*

4. Result & Discussion

4.1 Result

Context	Method	Factor	Literature
Information Security System	Attack Defense Model Game	Hardware Design, Software Design	[1]
Cloud Computing	Graph Neutral Method (GNN)	Cyber Threat Information (CTI)	[2]
Cloud Security	Homomorphic Encryption	Homomorphic Secret Sharing	[3]
Users Security	PMT (Protection Motivation Theory)	Information Security Behavior of Individuals, Routine activity and Information Security, Online Activities and Malware Infection, Software Installed	[4]
Information Security	PMT (Protection Motivation Theory)	Self-Efficiency, Perceived impact of Potential Events	[5]
Cloud Computing	Provable Data Possession (PDP)	Noncryptographic and cryptographic techniques	[6]
Information Security	Information Security Method	Population, Comparison, Outcomes, Context	[7]
Cloud Computing	Testing and Evaluation Systems	Testing Environment, Evaluation Technology, Evaluation Services	[8]
Cloud Computing Networks	Graph Convolutional Neural Network and GraphSAGE models	Anomaly Detection, Adaptive Filtering, Behavior Modelling, Application of Game Theory, Service Allocation	[9]
Cloud Computing Security	Artificial Neural Network (ANN)	Training Data Quality, Network Architecture, Weight Adjustment Algorithms	[10]

4.2 Research context used for Information Security used on Cloud Computing

The research on Information Security in Cloud Computing focuses on several critical areas: the information security system[1], cloud computing security[3], user security[4], and cloud computing networks[9]. The information security system plays a vital role in safeguarding sensitive data from unauthorized access and cyber threats, ensuring that the integrity, confidentiality, and availability of information are maintained.

In the context of cloud computing, security measures are designed to protect the infrastructure and services that host and process vast amounts of data. User security is also a key concern, as the growing reliance on cloud services requires robust authentication and authorization mechanisms to ensure that only authorized users can access sensitive data. Additionally, cloud computing networks must be secured against vulnerabilities that could be exploited by cyber-attacks, ensuring that data transmission between clients and cloud servers remains protected. Collectively, these areas form the foundation of research aimed at improving the security landscape within cloud computing environments.

4.3 The method used for the adoption of Information Security

The method used for the adoption of Information Security in cloud computing incorporates a variety of advanced techniques and models to enhance security and protect sensitive data. The Attack Defense Model Game [1] is applied to simulate potential threats and defensive strategies, enabling a dynamic understanding of how attacks may unfold and how to counteract them effectively. Graph Neural Methods [2][9] and GraphSAGE [9] are utilized to analyze and learn from network structures, providing insights into security vulnerabilities within cloud networks by leveraging complex graph-based relationships. Homomorphic Encryption [3] allows for secure data processing in cloud environments, enabling computations on encrypted data without compromising privacy. Meanwhile, the Protection Motivation Theory [4] is employed to understand user behavior and motivations in adopting secure practices.

Emphasizing the psychological aspects of information security adoption. Provable Data Possession [6] ensures that cloud storage providers can verify data integrity without having direct access to the data itself, adding an extra layer of trust in cloud-based storage systems. Additionally, traditional Information Security Methods [7] are combined with Testing Evaluation Systems to rigorously

evaluate the effectiveness of security protocols. The integration of Artificial Neural Networks (ANN) [10] enhances the ability to detect and respond to anomalies in real-time, further strengthening the security framework. These methods collectively form a robust approach to the adoption of information security in cloud computing.

4.4 What factors influence uses Information Security on Cloud Computing

Several factors influence Information Security on Cloud Computing, spanning technical, behavioral, and procedural dimensions. Hardware and software design [1] Software design and hardware design are both essential for ensuring information security in cloud computing. Software design focuses on building secure systems and applications that run in the cloud, incorporating features like encryption, secure access controls, and real-time monitoring to protect data from unauthorized access or breaches. Software must be designed with security protocols in mind, ensuring secure coding, patch management, and robust logging to detect threats early. On the other hand, hardware design involves creating secure physical infrastructure, such as servers and processors, that safeguard the cloud environment. This includes using secure components like hardware-based encryption, and secure boot mechanisms to protect against both physical tampering and hardware-level vulnerabilities. Together, secure software and hardware designs provide a multi-layered defense, ensuring that both the virtual and physical components of cloud computing are resilient against cyber threats. form the foundation for secure systems, requiring robust architectures to resist cyber threats.

Cyber threat information plays a crucial role in predicting and preventing attacks, while homomorphic secret sharing enhances data privacy even during computation. Homomorphic secret sharing is a cryptographic technique that enhances data security in cloud computing by allowing sensitive information to be processed without revealing its actual content. It combines two methods: secret sharing, where data is divided into smaller pieces or "shares" and distributed across different locations, and homomorphic encryption, which enables calculations to be performed on encrypted data without needing to decrypt it. When applied in the cloud, homomorphic secret sharing allows cloud providers to carry out operations like data analysis or processing on the encrypted shares while keeping the original data hidden. This ensures that the cloud service never has access to the actual content, protecting it from unauthorized access or breaches. The technique is particularly valuable in cloud computing, where it guarantees that sensitive information remains private and secure, even when stored and processed on remote servers, enabling users to benefit from cloud services without compromising data security and privacy.

The information security behavior of individuals also significantly affects cloud security Information security behavior in cloud computing refers to the proactive steps and practices taken by individuals and organizations to protect sensitive data and ensure the safety of cloud environments. This behavior is especially important because cloud computing introduces unique challenges, such as storing data remotely, sharing infrastructure, and accessing services from various devices and locations. Key aspects of this behavior include using strong authentication methods, like complex passwords and multi-factor authentication (MFA), to prevent unauthorized access. Organizations should also implement strict access control measures, allowing only authorized users to access sensitive information. This includes using role-based access control (RBAC) and the principle of least privilege, where users are given the minimum permissions necessary for their roles. Additionally, encrypting data both when it is stored and while it is being transferred is crucial for protecting sensitive information, which requires effective encryption methods and secure handling of encryption keys.

However, despite the importance of these security behaviors, several challenges can make it difficult to maintain effective security measures. For instance, users may become complacent if they believe that the cloud is inherently secure, leading to risky behaviors. The complexity of different cloud services can also result in misconfigurations, putting sensitive data at risk. Furthermore, the shared responsibility model can create confusion regarding who is responsible for security, which can result in gaps in protection if organizations mistakenly think that their cloud provider handles all security concerns. Many organizations, especially smaller ones, may struggle to find the resources and expertise needed to implement strong security measures. To combat these issues, it is essential for organizations to promote a culture of security awareness by providing regular training and education about cyber threats. By taking a proactive and informed approach to security behaviors, organizations can significantly reduce risks associated with cloud computing and better protect their sensitive information, as actions such as poor security practices can introduce vulnerabilities. Additionally, routine activities and online behaviors are linked to increased risks of malware infections through unsafe interactions. The software installed and users' self-efficiency, their belief in managing security also play roles in securing cloud environments. This is coupled with their perception of the impact of potential threats, influencing their security behaviors. The adoption of both noncryptographic and cryptographic techniques ensures multi-layered protection. External factors like population size, comparison of security outcomes, and specific context in which cloud services are used affect security outcomes as well. Lastly, anomaly detection, behavior modeling, filtering techniques, training data quality, network architecture, and continuous evaluation through testing environments and evaluation services are crucial in identifying and mitigating emerging threats effectively. These factors collectively influence the adoption and effectiveness of information security strategies in cloud computing.

5. Conclusion

This research underscores the vital role of information security in cloud computing, particularly as organizations increasingly migrate sensitive data to cloud environments. The findings demonstrate that robust security measures anchored in securing systems, infrastructure, user authentication, and networks are essential to safeguarding sensitive information against evolving cyber threats. Advanced methodologies such as the Attack Defense Model, Graph Neural Networks, and Homomorphic Encryption have proven effective in addressing these threats, while user behavior and effective architectural design significantly influence security outcomes. Continuous evaluation and anomaly detection are vital for maintaining a resilient security posture in cloud environments. This study contributes valuable insights into the interplay between information security and cloud computing, equipping organizations and cloud service providers with practical strategies to enhance data protection and foster user trust.

Future research could explore the implications of emerging technologies such as artificial intelligence (AI) and machine learning (ML) on cloud security practices, investigating how these technologies can be leveraged to predict and mitigate security threats. Additionally, a deeper understanding of user behavior and its impact on cloud security could be explored through behavioral analytics studies, focusing on identifying patterns that lead to security breaches and developing training programs to improve user security practices. Investigating the influence of regulatory frameworks on the adoption of security measures in cloud computing would provide insights into how compliance drives security practices across different industries. Furthermore, as more organizations adopt multi-cloud strategies, research could focus on developing comprehensive security frameworks that address the unique challenges associated with managing security across multiple cloud service providers. Lastly, examining how organizational culture and management practices affect the implementation and effectiveness of information security measures in cloud computing could yield valuable insights for practitioners. By addressing these areas, future research can further advance the understanding of information security within cloud computing and contribute to developing more effective security strategies and frameworks.

References

1. Liu, Y., Wang, Q., Zheng, Z., & Cui, L. (2024). Control modeling and optimization of network information security system based on deep learning data interaction. *Measurement Sensors*, *33*, 101221. https://doi.org/10.1016/j.measen.2024.101221
2. Mohammed, S., Nanthini, S., Krishna, N. B., Srinivas, I. V., Rajagopal, M., & Kumar, M. A. (2023). A new lightweight data security system for data security in the cloud computing. *Measurement Sensors*, *29*, 100856. https://doi.org/10.1016/j.measen.2023.100856
3. Ali, S., Wadho, S. A., Yichiet, A., Gan, M. L., & Lee, C. K. (2024). Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing. Egyptian Informatics Journal, 27, 100519. https://doi.org/10.1016/j.eij.2024.100519
4. Arenas, Á., Ray, G., Hidalgo, A., & Urueña, A. (2023). How to keep your information secure? Toward a better understanding of users security behavior. Technological Forecasting and Social Change, 198, 123028. https://doi.org/10.1016/j.techfore.2023.123028
5. Hooper, V., & Blunt, C. (2019). Factors influencing the information security behaviour of IT employees. Behaviour and Information Technology, 39(8), 862–874. https://doi.org/10.1080/0144929x.2019.1623322
6. Hindawi. (2023). Retracted: The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges—A Systematic Literature Review (SLR). *Computational Intelligence and Neuroscience*, *2023*, 9838129. https://doi.org/10.1155/2023/9838129
7. INFORMATION SECURITY CULTURE: A SYSTEMATIC LITERATURE REVIEW. (2015). *Proceedings of the 5th International Conference on Computing and Informatics*, *205*. https://soc.uum.edu.my/icoci/2023/icoci2015/eProcsICOCI2015/PDF/PID205.pdf
8. Testing and Evaluation System for Cloud Computing Information Security Products. (2020). *Procedia*, *84–87*(166). https://www.sciencedirect.com/science/article/pii/S1877050920301459
9. Abdullayeva, F., & Suleymanzade, S. (2024). Cyber Security Attack Recognition on Cloud Computing Networks Based on Graph Convolutional Neural Network and GraphSage models. Results in Control and Optimization, 15, 100423. https://doi.org/10.1016/j.rico.2024.100423
10. Hasimi, L., Zavantis, D., Shakshuki, E., & Yasar, A. (2024). Cloud Computing Security and Deep Learning: An ANN approach. Procedia Computer Science, 231, 40–47. https://doi.org/10.1016/j.procs.2023.12.155
11. Maf'ul, T. A. U. F. I. Q., Rangkuti, M. I., (2023). Analysis Of Information Technology Implementation And Information Security Awareness (Isa) Regarding Financial Reporting (Overview With The Data Protection Laws By The European Union's General Data Protection Regulation (Gdpr). *Russian Law Journal*, *11*(6).
12. Syah, D. H., Muda, I., Lumbanraja, P., & Kholis, A. (2023). The Role of Cloud Computing on Accounting Information System Quality: A Study in Hotel Industry. *TEM Journal*, 12(3), 1890. https://www.temjournal.com/content/123/TEMJournalAugust2023_1890_1901.html
13. Sibuea, A.Y., Panjaitan, l.F, (2020). Protecting The Privacy of Customer's Personal In the Era of Cloud Computing. *Turkish Online Journal of Qualitative Inquiry*. 11(4). 741- 745. https://tojqi.net/index.php/journal/article/view/6716