SECURITY THREAT ANALYSIS IN CLOUD COMPUTING

Muhammad Iqbal Fadillah, Mohamad Irvan Zidni, Riko Adrian Maulana, Abdul Halim Anshor
Department of Informatics Engineering, Faculty of Engineering, Pelita Bangsa University, West Java, Indonesia
irvan.perkuliahan@gmail.com

ABSTRACT

Cloud computing provides significant benefits such as scalability, cost efficiency, and flexibility in accessing computing resources. However, its adoption introduces critical security challenges for organizations, necessitating a thorough analysis of associated risks. This research identifies and categorizes the primary security threats in cloud computing, including data loss, data leakage, cyberattacks, and unauthorized access, and evaluates their impact on organizational operations, data security, and regulatory compliance, with a focus on the financial and healthcare sectors. The study reveals that cyberattacks are the most prevalent and disruptive threat, while data leakage leads to significant legal repercussions and loss of trust. Practical recommendations include adopting encryption, multi-factor authentication, and strict access controls, as well as complying with industry standards like PCI DSS for finance and HIPAA for healthcare. Additionally, a comprehensive risk management framework comprising risk identification, assessment, mitigation, and continuous monitoring is proposed to enhance organizational resilience. By implementing these strategies, organizations can securely leverage cloud computing, maintain regulatory compliance, protect sensitive data, and uphold customer trust.

Keyword : *Cloud Computing Security, Security Threats*

1. INTRODUCTION

Cloud Computing technology has become one of the dominant trends in the information and communication technology (ICT) industry in recent years. Cloud Computing provides various advantages, such as the ability to scale, cost efficiency, and flexible access to computing resources. However, behind these benefits, there are also significant security threats that need to be taken seriously. Data security and privacy are important issues for individuals and organizations using Cloud Computing services, so managing security risks is crucial. Failure to manage these risks can lead to serious consequences, such as sensitive data leakage, operational disruption, and loss of customer trust. This research aims to provide a thorough analysis of the security threats associated with the use of Cloud Computing, considering both organizational and risk management perspectives. It will also focus on specific sectors, such as finance or healthcare, to generate more specific and relevant insights.

Several previous studies have explored various aspects of security in Cloud Computing. (Subashini and Kavitha)[1] analyzed security challenges in Cloud Computing, including data security, privacy, and compliance issues. Their research emphasized the importance of data encryption, strong authentication, and proper access control to protect sensitive data in cloud environments. On the other hand, (Hashizume et al.)[2] proposed a security framework to support data privacy in Cloud Computing through encryption and access control tailored to organizational policies.

Although previous research provides valuable insights into security threats in Cloud Computing, there are still some gaps that need to be addressed. Most of these studies put more emphasis on technical aspects, such as encryption and access control, but less on addressing security challenges from an organizational and risk management perspective. In addition, many studies were conducted in a general context, without considering the specific needs and challenges of a particular industry.

As an increasing number of organizations adopt Cloud Computing, it is important to understand the security threats inherent in this technology. Failure to manage security risks can result in negative impacts, such as sensitive data leakage, operational disruption, loss of customer trust, fines from regulators, and potential litigation.

Therefore, the main objective of this research is to analyze the security threats in the use of Cloud Computing technology from an organizational and risk management perspective. This research aims to identify and categorize the main security threats associated with the use of Cloud Computing in an organizational context, and analyze the potential impact of these threats on operations, data security, and regulatory compliance. In addition, this research will provide practical recommendations for managing and mitigating security risks, taking into account the specific needs and challenges of the sectors studied, and provide a comprehensive risk management framework to support secure and effective Cloud Computing deployments.

The adoption of Cloud Computing technology by organizations continues to increase along with the demand for scalability and cost efficiency. While Cloud Computing offers many benefits, it also brings significant security risks, especially related to data security and privacy. When data is stored and processed in a cloud environment managed by a third party, organizations are at risk of sensitive data leakage, unauthorized access, and privacy breaches, which can result from misconfiguration, cyberattacks,

or unethical actions by the cloud service provider or its employees.

Research conducted by Subashini and Kavitha has highlighted the security challenges in Cloud Computing, including data security, privacy, and compliance issues. They emphasized the need for data encryption, strong authentication, and proper access control to protect sensitive data in the cloud environment. However, the focus of this research is more on technical aspects and less on security challenges from an organizational and risk management point of view.

Meanwhile, (Hashizume et al.) [2] proposed a security framework to protect data privacy in Cloud Computing through encryption and access control tailored to organizational policies. Despite providing contextual solutions, these studies are still general in nature and have not considered the specific needs and challenges of a particular sector.

One of the identified gaps is the lack of research that addresses security threats in Cloud Computing from an organizational and risk management perspective. Most previous research has focused on technical aspects, such as encryption and access control, without considering the potential impact on organizational operations, data security and regulatory compliance.

A clear example of the impact of security threats in Cloud Computing is the data leak incident experienced by health insurance company Anthem Inc. in 2015, which resulted in the leak of personal data and medical information of nearly 79 million people. This incident emphasized the importance of managing security risks in the use of Cloud Computing, especially in sensitive sectors such as healthcare.

Most of the previous research was conducted in a general context without considering the specific needs and challenges of a particular industry or sector. Each sector has different security requirements and regulations; for example, the financial sector has stricter security standards than other sectors to protect sensitive data and transactions.

With more and more organizations adopting Cloud Computing, it is important to understand the security threats that come with it. Failure to manage security risks can lead to adverse consequences, including sensitive data leakage, operational disruption, loss of customer trust, fines from regulators, and potential lawsuits.

Therefore, this research aims to provide an in-depth analysis of the security threats associated with the use of Cloud Computing, taking into account both organizational and risk management perspectives, as well as focusing on specific sectors, such as finance or healthcare, to provide more specific and relevant insights.

Threats include data leaks, cyberattacks, misconfigurations, and other security incidents that can affect an organization's operations, data security, and regulatory compliance.

Furthermore, this research will analyze the potential impact of such security threats in detail. For instance, the impact of sensitive data leaks not only results in loss of customer trust but can also lead to significant fines from regulators and lawsuits that can threaten business continuity. Operational disruptions due to security incidents can also cause huge financial losses and reduce productivity.

By understanding the potential impact of security threats, organizations can take proactive measures to mitigate the risks. This research will provide practical recommendations for managing and mitigating security risks in the use of Cloud Computing, which will take into account the specific needs and challenges of the sectors studied, such as finance or healthcare, which have strict security regulations and standards.

For example, in the financial sector, protecting transaction data and customers' personal information is a top priority, so security recommendations should include end-to-end data encryption, multi-factor authentication, and strict access control. In the healthcare sector, protecting patient data and the confidentiality of medical information is a key focus, so security recommendations should comply with regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the United States.

In addition to providing practical recommendations, this research will also develop a comprehensive risk management framework to support the secure and effective implementation of Cloud Computing in organizations. This framework will include processes of risk identification, risk assessment, risk mitigation, and ongoing risk monitoring, which will help organizations make better decisions regarding the use of Cloud Computing by considering security risks and their impact on the business.

With this research, it is hoped that organizations can gain a better understanding of the security threats in the use of Cloud Computing, as well as effective strategies to manage these risks. Thus, organizations can utilize Cloud Computing more securely and in compliance with applicable regulations, while still protecting sensitive data and maintaining customer trust.

By analyzing security threats from an organizational point of view, this research will identify and categorize the main threats associated with the use of Cloud Computing in an organizational context. These include threats such as data leaks, cyber-attacks, misconfigurations, and other security incidents that can impact an organization's operations, data security, and regulatory compliance.

Furthermore, this research will explore the potential impact of such security threats in depth. For example, sensitive data leaks not only result in loss of customer trust but can also lead to hefty fines from regulators and lawsuits that threaten an organization's business continuity. Operational disruptions due to

security incidents can also lead to significant financial losses and lower productivity.

By understanding the potential impact of security threats, organizations can take proactive measures to mitigate such risks. Therefore, this research will provide practical recommendations for managing and mitigating security risks in the use of Cloud Computing. These recommendations will take into account the specific needs and challenges of the sectors studied, such as finance or healthcare, which have strict security regulations and standards.

For example, in the financial sector, protection of transaction data and customers' personal information is a top priority, so security recommendations should include end-to-end data encryption, multi-factor authentication, and strict access control. On the other hand, in the healthcare sector, protection of patient data and confidentiality of medical information should be the main focus, so security recommendations should comply with regulations such as HIPAA in the United States.

In addition, this research will also develop a comprehensive risk management framework to support the secure and effective implementation of Cloud Computing in organizations. This framework will include the processes of risk identification, risk assessment, risk mitigation, and continuous risk monitoring, which will assist organizations in making decisions regarding the use of Cloud Computing by considering security risks and their impact on business.

With this research, it is expected that organizations can gain a deeper understanding of the security threats in using Cloud Computing, as well as effective strategies to manage these risks. Thus, organizations can utilize Cloud Computing more securely and comply with applicable regulations, while still protecting sensitive data and maintaining customer trust.

2. LITERATURE REVIEW

In analyzing the security threats associated with the use of Cloud Computing technology, it is important to understand the previous research that has been done in this area. Several studies have explored various aspects of security in Cloud Computing and provided valuable insights.

Subashini and Kavitha have conducted a survey on security issues in Cloud Computing service delivery models. They identified key challenges related to security, including data security, privacy, and regulatory compliance. This research emphasizes the importance of data encryption, implementation of strong authentication, and proper access control settings to protect sensitive data in the cloud environment. In addition, they also discuss the issue of compliance with applicable regulations and standards in various industry sectors (Subashini & Kavitha) [1].

Meanwhile, Hashizume et al. proposed a security framework aimed at protecting data privacy in Cloud Computing. This framework includes the implementation of data encryption as well as access control tailored to the organization's policies. This research emphasizes the importance of maintaining data confidentiality and integrity in a cloud environment by using appropriate security mechanisms. In addition, they also discuss challenges related to encryption key management and user authentication processes (Hashizume et al.) [2].

On the other hand, research by Gonzalez et al. focused on analyzing security risks in Cloud Computing. They developed a methodology to identify and evaluate security risks related to the use of cloud services. This methodology considers various factors, such as the type of cloud service, data criticality, and the service provider's ability to handle security risks. This research provides practical guidance for organizations in managing security risks in cloud environments (Gonzalez et al.) [3].

Although these studies provide valuable insights, most of them focus more on technical aspects or are general in nature, without regard to the specific needs and challenges of a particular industry or sector. In addition, some studies lacked addressing security threats from an organizational and risk management perspective.

In this study, researchers seek to analyze security threats in the use of Cloud Computing technology from an organizational and risk management perspective. The focus of this research will also be on specific sectors, such as the financial or healthcare sectors, to provide more specific and relevant insights. Thus, this research is expected to make a new contribution to the understanding of security threats in Cloud Computing as well as their management strategies in the context of specific organizations and industry sectors.

3. RESEARCH METHODS

This research adopts a qualitative approach using the literature study method and secondary data analysis. The following are the steps taken in this research:

3.1. Literature Review

At this stage, an in-depth literature review was conducted regarding security threats related to the use of Cloud Computing technology. This review includes journal articles, books, research reports, and other relevant sources. The goal is to analyze and identify previous research, explore key concepts, and find gaps or deficiencies in the existing literature.

3.2. Secondary Data Collection

The next step is to collect secondary data from reliable sources, such as industry reports, case studies, and security incident reports. This secondary data is used to analyze security threats that occur in the practice of using Cloud Computing and their impact on organizations.

3.3. Data Analysis

The data obtained from the literature review and secondary sources will be thoroughly analyzed using the content analysis method. In this stage, researchers will identify, categorize, and interpret the main security threats that arise in the use of Cloud Computing.

3.4. Supporting Tools and Software

In this research, common software such as qualitative data analysis tools (e.g. NVivo or ATLAS.ti) and word processing applications (Microsoft Word) are used to support the analysis and writing process.

3.5. Experimental Design and Sampling Technique

This research did not involve any direct experiments or trials. Sampling techniques were not specified because the nature of the research was qualitative and did not involve direct sampling. However, the selection of secondary data sources was purposive based on their relevance and credibility.

3.6. Data Testing and Analysis Plan

Data analysis will be conducted using the content analysis method, which includes systematic coding, categorizing, and interpreting the data. This research does not use a specific statistical model, but rather applies qualitative data analysis techniques that are in line with the research objectives.

3.7. Validation and Triangulation

To ensure the validity and reliability of the research results, a data validation and triangulation process was conducted. Validation was done by comparing the research results with literature and other relevant sources. Triangulation is done by involving experts or practitioners in the field of Cloud Computing security to provide input and feedback on the research results.

Table 1: Examples of Security in Cloud Computing

Threat category	Description
Data loss	Loss of data or access to data due to misconfiguration, device malfunction, or cyberattack.
Data leakage	Leakage of sensitive data due to security breach misconfiguration, or unauthorized access.
Cyberattack	Cyberattacks such as distributed denial of service (dd0s), malware, or vulnerability exploitation.
Unauthorized access	Unauthorized accesss to cloud data or systems by unauthorized parties

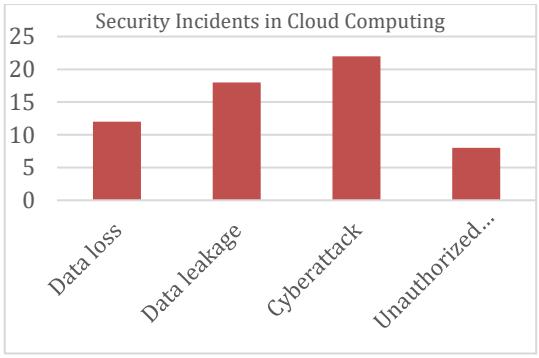

Figure 1.Security incidents in cloud computing by threat category

The graph shown in Figure 1 depicts the number of security incidents in Cloud Computing by threat category. The horizontal axis (x-axis) in the graph represents the security threat categories, namely Data Loss, Data Leakage, Cyber Attack and Unauthorized Access. While the vertical axis (y-axis) shows the number of security incidents that occur in each category.

From the graph, it can be seen that the threat category with the highest number of incidents is Cyber Attack, with 22 recorded incidents. This shows that cyberattacks, such as Distributed Denial of Service (DDoS), malware, or vulnerability exploitation, are a significant threat in the use of Cloud Computing.

The next threat category that had the highest number of incidents was Data Leakage, with 18 recorded incidents. This indicates that sensitive data leakage due to security breaches, misconfiguration, or unauthorized access is a major concern in Cloud Computing security.

Next, there were 12 incidents related to Data Loss, which can be caused by factors such as misconfiguration, device damage, or cyberattacks that lead to data loss or access to data.

The threat category with the lowest number of incidents was Unauthorized Access, with 8 recorded incidents. Although the number is lower than other categories, unauthorized access to cloud data or systems by unauthorized parties is still a threat that needs to be considered.

Visualizing the data in this format provides a clear picture of the distribution of security incidents in Cloud Computing by threat category. This information can assist organizations in determining priorities and strategies for managing security risks associated with the use of Cloud Computing.

4. RESULTS AND DISCUSSION

In this study, researchers explored security threats related to the use of Cloud Computing technology from an organizational and risk management perspective. This research also focused on the financial and healthcare sectors to provide a more in-depth and relevant understanding. Based on the literature review and secondary data analysis, several important scientific findings were identified.

4.1. Major Security Threats in Cloud Computing Usage

One of the key findings of this research is the identification and clustering of significant security threats in organizations' use of Cloud Computing. Through data analysis, the researcher grouped the security threats into four main categories: data loss, data leakage, cyberattacks and unauthorized access.

4.1.1. Data Loss

Loss of data or access to data in the context of Cloud Computing can be caused by a variety of factors, such as misconfiguration, device malfunction, or cyberattacks (Armbrust et al.) [4].

Data loss can have a major impact on an organization, including operational disruption, loss of productivity, as well as significant financial losses.

4.1.2. Data Leakage

Sensitive data leakage is one of the most worrying security threats in the context of Cloud Computing. Leaks can result from security breaches, misconfigurations, or unauthorized access by unauthorized parties. The consequences of these leaks can include loss of customer trust, fines from regulators, and potential lawsuits that threaten the viability of the organization.

4.1.3. Cyber Attacks

Cyberattacks, such as Distributed Denial of Service (DDoS), malware, or vulnerability exploitation, are significant threats in the use of Cloud Computing (S. Rashid) [5]. These attacks can cause service disruptions, data loss, or even system hacking and theft of sensitive information.

4.1.4. Unauthorized Access

Unauthorized access to cloud data or systems by unauthorized parties is also a security threat that needs attention (Mather et al.) [6]. This can occur as a result of misconfiguration, system vulnerabilities, or deliberate actions from internal or external parties attempting to access data illegally. These findings provide a clear understanding of the major security threats faced by organizations using Cloud Computing. By understanding these threats, organizations can take the necessary steps to manage and mitigate security risks.

4.2. The Potential Impact of Security Threats on Organizations

This research also analyzed the potential impact of security threats on organizations using Cloud Computing. This impact may vary depending on the type of threat and the industry sector involved.

4.2.1. Impact on Organization Operations

Security incidents in Cloud Computing, such as data loss, cyberattacks, or unauthorized access, can result in significant operational disruptions for organizations. This can lead to reduced productivity, delays in service, and even temporary suspension of business activities. These impacts often result in large financial losses and can damage an organization's reputation.

4.2.2. Impact on Data Security and Privacy

Threats such as data leakage or unauthorized access to sensitive data can compromise data security and privacy for both organizations and customers or other related parties (Alzain et al.) [7].

In the financial sector, leakage of transaction information and personal data of customers can lead to loss of customer trust and fines from regulators. Meanwhile, in the healthcare sector, leakage of patient information and medical data can violate regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the United States, potentially resulting in serious legal consequences.

4.2.3. Impact on Regulatory Compliance

Security incidents in Cloud Computing can also impact an organization's compliance with regulations and standards applicable in certain industry sectors. For example, in the financial sector, there are strict security standards to protect sensitive financial data and transactions, such as the Payment Card Industry Data Security Standard (PCI DSS). Non-compliance with these standards can result in heavy fines and other sanctions.

These findings emphasize the importance of understanding the potential impact of security threats in Cloud Computing, not only from a technical perspective but also in terms of organizational operations, data security, and compliance with relevant regulations. By understanding such impacts, organizations can take appropriate actions to manage risks and mitigate adverse consequences.

4.3. Practical Recommendations for Managing Security Risks in Cloud Computing

Based on the analysis and findings of this study, the researcher provides practical recommendations for managing security risks in the use of Cloud Computing, taking into account the specific needs and challenges of the financial and healthcare sectors.

4.3.1. Recommendations for the Financial Sector

End-to-End Data Encryption: Protection of financial transaction data and customers' personal information is a top priority. Therefore, end-to-end data encryption is essential to prevent data leakage during transmission and storage (S. Lian,) [8].

Multi-Factor Authentication: To improve the security of access to sensitive systems and data, financial organizations need to implement multi-factor authentication, which can be a combination of passwords, security tokens, or biometrics (S. Sedky and H. Riad) [9].

Role-Based Access Control: The implementation of role-based access control (RBAC) allows restricting access to data and systems to authorized users only, according to their roles and responsibilities within the organization (Zissis & Lekkas) [10].

Compliance with Security Standards: Financial organizations must comply with relevant security standards, such as PCI DSS, to ensure the protection of financial data and sensitive transactions.

4.3.2. Recommendations for the Healthcare Sector

Encryption of Patient Data: To maintain the confidentiality of patients' medical information, encryption of patient data is essential in the context of Cloud Computing in the healthcare sector (Gholami & Laure) [11].

Strict Access Control: Implementation of strict access controls and restriction of access only to authorized medical personnel is essential to maintain the privacy of patient data and comply with regulations such as HIPAA.

Security Auditing and Monitoring: Healthcare organizations need to conduct regular security audits and monitoring to detect potential security incidents or unauthorized access to patient data.

Security Awareness Training: Providing security awareness training to medical staff and other employees can improve understanding of security risks as well as best practices in managing patient data securely (R. K. Banyal, V. K. Jain) [12].

Compliance with HIPAA Regulations: Healthcare organizations must ensure compliance with HIPAA regulations and other related security standards to protect patient data and avoid legal consequences.

These recommendations provide practical guidance for organizations in the financial and healthcare sectors on managing security risks in the use of Cloud Computing. By implementing these recommendations, organizations can improve the protection of sensitive data, comply with applicable regulations, and reduce the risk of security incidents that could negatively impact the business.

4.4. Security Risk Management Framework for Cloud Computing

In addition to providing practical recommendations, this research also proposes an overarching security risk management framework to support the secure and effective implementation of Cloud Computing within organizations. This framework includes the processes of risk identification, risk assessment, risk mitigation and ongoing risk monitoring.

5. CONCLUSION

This research successfully identified key security threats in cloud computing, including data loss, data leakage, cyberattacks, and unauthorized access, and analyzed their impacts on organizational operations, data security, and regulatory compliance, particularly in the financial and healthcare sectors. The findings revealed that cyberattacks are the most frequent and disruptive, while data leakage poses significant legal and trust implications, emphasizing the importance of tailored risk management strategies. Practical recommendations include the adoption of encryption, multi-factor authentication, and strict access controls, as well as compliance with industry-specific standards like PCI DSS for finance and HIPAA for healthcare. Additionally, a security risk management framework encompassing risk identification, assessment, mitigation, and continuous monitoring was proposed to enhance organizational preparedness and response to security incidents. By implementing these strategies, organizations can leverage the benefits of cloud computing securely while maintaining compliance and safeguarding sensitive data. For future research, it is recommended that case studies or practical implementations of the recommendations and frameworks proposed in this research be conducted in specific organizations or sectors. This will provide empirical validation and enable further refinement based on real-life experiences. In addition, further research can also be conducted to explore security threats arising from new technology trends, such as the Internet of Things (IoT) and edge computing, in the context of Cloud Computing.

REFERENCES

[1] Subashini, S., & Kavitha, V., *A survey on security issues in service delivery models of Cloud Computing. In Journal of Network and Computer Applications*, vol. 34, no. 1, 2011.

[2] Hashizume, K., Rosado, D. G., Fernández Medina, E., & Fernandez, E. B., *An analysis of security issues for Cloud Computing. Journal of Internet Services and Applications*, vol. 4, no. 1, 2013.

[3] Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M., & Pourzandi, M., *A quantitative analysis of current security concerns and solutions for Cloud Computing. Journal of Cloud Computing*, vol. 1, no. 1, 2012.

[4] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., & Stoica, I., *of Cloud Computing*, 2010.

[5] S. Rashid., *The Security Threats in Cloud Computing*, vol. 1, no. 4, 2020.

[6] Mather, T., Kumaraswamy, S., & Latif, S., *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, vol. 1, 2009.

[7] Alzain, M. A., Soh, B., & Pardede, E., *MCDB : Using Multi-clouds to Ensure Security in Cloud Computing MCDB : Using Multi Clouds to Ensure Security in Cloud Computing*, 2011.

[8] S. Lian., *"Multimedia Cloud Computing and IoT: Security Issues," in Multimedia Cloud Computing.*, 2020.

[9] S. Sedky and H. Riad., *Towards Enhancing Cloud Security: Computing Multi-Factor Authentication for Securing Mobile User's Data. International Conference on Computer and Applications (ICCA)*, pp. 119-124, 2018

[10] Zissis, D., & Lekkas, D., *Addressing Cloud Computing security issues. Future Generation Computer Systems*, vol. 28, no. 3, 2012.

[11] Gholami, A., & Laure, E., *SECURITY AND PRIVACY OF SENSITIVE DATA IN CLOUD COMPUTING : A SURVEY OF RECENT DEVELOPMENTS*, pp. 131-150, 2015

[12] R. K. Banyal, V. K. Jain, and P. K., *"Security Issues in Cloud Computing," in Cybersecurity and Secure Information Systems*, 2019