JURNAL SYNTAX ADMIRATION

Syntax Admiration: p-ISSN 2722-7782 | e-ISSN 2722-5356 Vol. 5, No. 11, November 2024

Data Security and Data Protection in Cloud Privacy Systems

Harson Kapoh[1], Putri Aprilyana[2] , Yeremia Julio Rafael Sumampow[3] , Marsya Priskila Mailake[4] , Farel Hizkia Manimpurung[5] , Hafizhan Qolby Pakaya[6]
[1,2,3,4,5,6] Politeknik Negeri Manado, Indonesia
Email: hvskapoh@gmail.com, putriaprilyana546@gmail.com, yeremiasumampouw3@gmail.com, achamarsya93@gmail.com, farelhizkia40@gmail.com, iganpakaya@gmail.com

Abstract

In this modern world, the internet has become very influential in our daily lives. The Internet has many uses to solve various problems, one of which is full hardware storage, therefore the Internet provides software-based data, for example, cloud storage applications. The study aims to analyze and evaluate various data security techniques and protection methods used in the cloud computing framework, focusing on vulnerability identification, risk mitigation strategy assessment, and user security awareness improvement. In addition, this study aims to analyze data security techniques and data protection approaches applied to cloud systems. In addition, the study also assesses potential risks and mitigates security threats such as cyberattacks and data breaches. Using qualitative methodologies, the study investigated relevant literature, examined real-life cases of data breaches, and analyzed the effectiveness of security measures such as encryption and multi-factor authentication. The findings show that cloud systems remain vulnerable to cyber threats like DDoS attacks, credential theft, and data breaches due to inadequate security protocols. Key recommendations include adopting encryption, improved multi-factor authentication practices, and encouraging collaboration between cloud service providers and users to strengthen data security. The research contributes by proposing a comprehensive approach to improving data protection in cloud environments, ensuring a secure and resilient infrastructure for users. Implementing these findings will support the development of more secure cloud technologies and increase user confidence in data security practices. It is hoped that the study's results can provide recommendations to improve data security and data protection in cloud systems.

Keywords: data, security, protection, cloud computing, cyber attacks.

Introduction

The development of data in recent decades has resulted in a major change in how information is managed, stored, and accessed (Hashem et al., 2015). In this sophisticated era, data has become a very profitable resource, not only for humans but also for companies and organizations around the world. Information is used as a basis for important decision-making, technology development, and increasing operational effectiveness (Sudiantini et al., 2023). As the volume of information generated every day proliferates, conventional approaches to information capacity and management face limitations, both in terms of flexibility and expected effectiveness. Therefore, there is an urgent need for more flexible and rapid innovation. One of the most progressive developments that addresses this need is cloud computing. Cloud computing provides a platform that allows information storage and processing remotely via the Web, without the need for complex hardware frameworks on the client side (Ali et al., 2015). Through cloud-based solutions, both businesses and individuals can access mechanical resources quickly and productively, with a better level of flexibility compared to conventional frameworks.

The global expansion of cloud computing technology has transformed the way data is managed, accessed, and protected across a wide range of industries. (Hasanah & Dinalestari Purbawati, 2024; Sun et al., 2014). As digital transformation accelerates, concerns about data security and privacy in cloud environments are becoming more urgent. Cyber threats, including data breaches, unauthorized access, and cyberattacks, are increasing significantly, posing a critical risk to the data of individuals and organizations around the world. With the increasing adoption of cloud computing, maintaining the integrity, availability, and confidentiality of data in cloud environments is an ever-growing global priority.

One of the advantages of cloud computing is its flexibility, which allows clients to change information capacity and prepare capacity according to their increasing needs. (Nasution, 2023). This provides significant efficiencies, as organizations do not have to invest heavily in computer equipment and programs that may not always be used to their full potential. (Ula, 2019). Additionally, the cloud offers ease of access, allowing users to access their information anytime and from anywhere, as long as there is an internet connection. The use of cloud computing has also driven digital transformation in businesses. Many sectors, from financial services, healthcare, and education, to government, have adopted the cloud to support their operations. (Al-Ruithe et al., 2018). The cloud is the foundation for other cutting-edge innovations, such as artificial intelligence (AI), big data, and the Internet of Things (IoT), which are increasingly important in creating innovative solutions and increasing the efficiency of forms of commerce (George et al., 2023). With the cloud, companies can grow faster, react more nimbly to market changes, and scale their operations globally without being tied to a physical framework (Dunggio & Fuad, 2023).

In line with the research conducted by Yang et al., (2020) stated that the continued growth of data storage pressure is driving the rapid development of the entire storage market due to the big data generated. By providing data storage and management, cloud storage systems are an integral part of the new era. Today, governments, enterprises, and individual users are actively migrating their data to the cloud. Huge amounts of data can result in tremendous wealth. The research presents a unique approach by integrating a multi-faceted assessment of the latest data security practices specific to the cloud environment, combining technology and organizational perspectives. The study identifies gaps in existing research, particularly in comprehensive strategies that can be universally applied across multiple industries to improve data protection.

The study introduces an integrated approach to evaluating data security practices, with a particular focus on the effectiveness of cloud protection strategies in mitigating modern cyber threats (Ogborigbo et al., 2024; Oladoyinbo et al., 2023). By assessing technical and organizational factors, the study offers a comprehensive analysis that bridges the current cloud data security research gap, with insights tailored to the latest technological advancements.

With the exponential growth in cloud computing adoption across various sectors, the need to create a secure cloud environment has become critical (Singh et al., 2016; Sunyaev & Sunyaev, 2020). Organizations, especially those in highly regulated sectors such as finance and healthcare, need a rigorous data protection framework to comply with privacy regulations and avoid heavy sanctions. Ensuring data security in a cloud environment is vital to support operational scalability without sacrificing user trust or compliance requirements.

The main objective of this study is to analyze the effectiveness of current security and data protection techniques in cloud computing systems and identify best practices that can reduce the risk of data breaches. The study also aims to put forward practical recommendations to improve cloud security strategies, ensuring the integrity, confidentiality, and availability of data across various cloud environments.

The research is beneficial to industry stakeholders by providing valuable insights into the strengths and limitations of existing cloud security protocols, as well as offering a framework that organizations can adopt to improve their data protection practices. In addition, the research contributes to the academic field by expanding the knowledge base on cloud security threats, paving the way for further study related to more advanced data protection technologies in cloud computing.

Research Methods

This research method uses a descriptive qualitative approach that aims to explore data security techniques and protection methods applied in cloud systems. This approach was chosen to allow for an in-depth analysis of the various security techniques that exist and to understand the frameworks used in mitigating risks in cloud environments. The study focuses on relevant literature, including scientific journals, technical articles, and case study reports related to data security breaches. In addition, this study examines real-life examples of data breaches in cloud systems to identify common security gaps and evaluate the effectiveness of the protection strategies implemented.

Data collection was carried out through a comprehensive literature search and document analysis on related case studies. These secondary data sources include previous research on cloud data security, technology company reports, and security standards from international organizations. Data analysis is carried out using thematic analysis methods, where the data obtained is outlined based on key themes such as encryption, multi-factor authentication, and cyber threat mitigation. Through this analysis, this study identifies patterns and best practices that can be used as recommendations for organizations to improve data security in cloud systems.

This investigation uses a subjective strategy consisting of several stages of in-depth investigation. First of all, this investigation begins with a comprehensive reflection of the writings, various thoughts, journal articles, and special reports related to cloud security innovations and information security approaches that are analyzed. This writing survey was conducted to gain an in-depth understanding of the subject of cloud security, subsequent improvements in related innovations, and information security methodologies that have been implemented by various businesses. The sources used include scientific journals, white papers from cloud suppliers, and rules and benchmarks issued by universal organizations such as ISO.

After the writing survey, this investigation continues with an investigation of subsequent cases of information breaches that occurred in the cloud framework. The cases were selected based on their relevance to the subject of cloud security, which includes various types of breaches such as personal information leaks, cyber-attacks, and framework vulnerabilities. Each case is analyzed to identify the points of weakness or vulnerability in the cloud framework that allowed the breach to occur. This investigation not only focuses on the technical point of view of the breach but also considers the organizational components, as well as the security approach.

Results and Discussion

The findings from this examination uncovered various vulnerabilities in cloud frameworks and recognized several common security dangers faced by cloud clients and benefit suppliers. These considerations provide a deep dive into the key challenges faced by the industry in securing information and foundations in cloud situations, and the steps that can be taken to mitigate these dangers. The key findings are further detailed below:

1. **Cyberattacks Against Cloud Frameworks**
   Cyberattacks targeting cloud frameworks are extensive, encompassing attacks such as Conveyed Dissent of Benefit (DDoS) attacks, hacking, credential theft, and zero-day vulnerability abuse Rachmad et al., (2023). These attacks compromise the acuity, accessibility, and confidentiality of information stored in the cloud. With the increasing choice of cloud innovation for businesses, the cloud has become a prime target for cybercriminals. The impact is felt not only by cloud service providers but also by clients, especially those with weak or helpless security arrangements. This shows that the cloud can be a very dangerous environment if not handled with the right precautions.
2. **The Need for Client Awareness of Top-Notch Security Many cloud services**
   Clients are not fully aware of the importance of implementing proper security measures, which ultimately worsens the overall security situation. Clients often overlook several important aspects of advanced security, such as frequently updating software, using strong and unique passwords, and understanding and implementing restricted access methods. In addition, they often fail to enable additional security options offered by cloud service providers, such as encryption or multi-factor security features. This lack of awareness opens up opportunities for cybercriminals to exploit vulnerabilities in systems that are not properly

secured. More serious preparation about the importance of security and anticipating cyber attacks will greatly assist clients in protecting their data from attacks.

3. **Security Measures: Encryption and Multi-Factor Verification**
   The rationale highlights the importance of certain security measures that have been shown to be effective in mitigating risks, such as information encryption and the implementation of Multi-Factor Authentication (MFA). Encryption, which ensures information from unauthorized access both while stored and in transit, is one of the most important measures in keeping sensitive data secure in the cloud. Multi-factor authentication, on the other hand, provides an additional layer of assurance by requiring a different authentication strategy at some point before a client can access the framework or information. The combination of these two strategies has been shown to completely mitigate the potential for unauthorized access and maintain the confidentiality of information, even if a client's credentials are successfully stolen.
4. **Collaboration between Service Providers and Clients**
   The rationale also highlights the importance of close collaboration between cloud service providers and clients to increase awareness and use of security measures. While providers must provide a secure foundation, clients also have a primary responsibility in securing their settings and accessing their information. With a collaborative approach, providers and clients can distinguish between each other and address potential risks before they are misused by unscrupulous parties. Without proper coordination between the two parties, this danger is anticipated to continue to grow as the adoption of cloud innovation becomes more widespread across various industry segments, including the government segment which is increasingly dependent on the cloud for large-scale information administration.
5. **Security Challenges in Tightly Controlled Segments Highly**
   Controlled sectors, such as the monetary, healthcare, and government segments, face extra challenges in accepting cloud administration. In these divisions, in addition to general cyber dangers, they also need to comply with various strict information security measures and directives. Failure to comply with these directives can result in very large fines or sanctions. In this way, the selection of cloud administration in these divisions must be done very carefully, guaranteeing that the cloud service provider complies with significant directives and provides appropriate security controls.

Discussion

The way to maintain data security and security in a cloud protection framework is to run approaches, forms, and technologies simultaneously (Rachmad et al., 2023). This combined approach is fundamental, as it allows organizations to strengthen information security and assurance in the cloud, reacting to an environment where cyber threats are always increasing. As we continue to rely on cloud capacity and handling, these fundamental security practices ensure that sensitive information remains protected, even as unused threats increase. To maintain information security and security in a cloud protection framework, there are several methodologies and best practices that can improve information security in a cloud situation. These include:

1. **Password**
   A strong password serves as the primary line of defense for securing a cloud account. An effective password should be a mix of upper and lower case letters, numbers, and

special characters, with a minimum recommended length of 12 characters. Changing passwords frequently is also a good idea, as it reduces the risk of theft or unauthorized access over time. Password managers are great instruments for storing and managing these complex passwords, allowing clients to follow the best patterns without having to remember each one separately.

2. **Multi-Factor Authentication (MFA)**
   Multi-factor authentication (MFA) adds a fundamental layer of security to every cloud account by requiring clients to provide additional authentication steps, such as entering a code sent via SMS or through an authenticator app. This security strategy ensures that even if a password is compromised, an attacker cannot effectively access the account without a second authentication step. For highly sensitive information or mission-critical frameworks, some organizations may implement more advanced MFA strategies, such as biometric displays or physical equipment tokens. These additional steps act as a boundary that significantly reduces the likelihood of unauthorized access.
3. **Information Encryption**
   Encryption is perhaps the most important innovation for maintaining the privacy of information in cloud environments. Through encryption, information is transformed into a structure that can only be accessed by those with the correct decryption key. Two important forms of encryption in the cloud framework are encryption in transit, which protects information as it is exchanged, and encryption at rest, which secures information stored in the cloud. End-to-end encryption is also gaining popularity, ensuring that information is scrambled from inception to storage, with only authorized parties able to access it. Encryption minimizes the chance of information leakage, securing sensitive data even if it is intercepted by unauthorized parties.
4. **Standard Inspections and Review**
   Continuous inspection of cloud activity is essential for finding signs of security breaches or unusual designs. Scheduled reviews allow security groups to proactively address potential threats and address vulnerabilities moments before an event can occur. Instruments for robotic inspection and log investigation provide a continuous, real-time view of cloud activity, which is critical for recognizing suspicious behavior and reacting quickly. Organizations can schedule regular reviews and assessments. to ensure this observation framework remains viable and aligned with the latest security guidelines, ensuring a strong line of defense against increasing dangers.
5. **Cloud Firewall**
   A cloud firewall acts as a defensive layer that prevents unauthorized access to information and applications stored in the cloud. Cloud firewalls block malicious activity, protect against potential vulnerabilities in applications, and anticipate API abuse. By designing firewall rules to coordinate an organization's risk profile, these firewalls provide a solid layer of security, especially when combined with a well-defined access management approach. An effective cloud firewall allows

organizations to more comprehensively restrict and monitor access, minimizing the exposure of sensitive information to outside threats.

6. **Information Security Settings**
   An information security approach is critical to the reliable and secure management of information in the cloud (Arafat, 2018). Organizations must determine what information can be stored in the cloud, as well as the security measures needed to ensure it is. This approach should include information storage, backup, deletion, and recovery methods to ensure compliance with security standards and controls. Organizations should routinely review and revise their information security approach to stay aligned with current best practices, and to adapt to changes in administrative requirements, security innovations, or where threats occur.
7. **Access Management and Identity Verification**
   Gain control over who can access specific assets within the cloud, typically through Role-Based Access Control (RBAC) (Younis et al., 2014). This approach ensures that people have access to only the information they need based on their role, reducing the potential for unauthorized access. Identity verification is also important in confirming that the person accessing a specific asset is who they claim to be. Together, these form a comprehensive framework for managing access, providing an extra layer of security that keeps sensitive information safe.
8. **Information Disaster Prevention (DLP) Tools**
   Information Disaster Prevention (DLP) tools are used to monitor and oversee the exchange of sensitive information. They offer help in recognizing and blocking any unauthorized attempts to share confidential data, either within the organization or remotely. DLP tools also offer help in complying with information security directives by anticipating information leaks. Additionally, they can identify and offer help in avoiding internal compromise by identifying suspicious activity and supporting information handling solutions. This makes DLP tools an essential part of a comprehensive information security in the cloud procedure.

Conclusion

Cloud computing offers tremendous benefits to individuals and businesses in terms of efficiency, uninterruptedness, and scalability, but data security remains the biggest challenge to overcome. The increasing security threats such as cyberattacks and hacking, as well as the increasing use of cloud services, require special attention to data security and protection. To ensure the security of data stored in the cloud, users must understand the right data protection strategy and implement comprehensive security measures. This includes using strict security policies and developing and implementing more advanced security and better encryption technologies to protect your data from evolving threats. In addition, it is also important to raise user awareness of the risks and potential threats so that they can better maintain data security in the cloud environment. With a proactive and sustainable approach, data storage in the cloud is a safe and reliable solution that allows users to enjoy the benefits of cloud computing without compromising security. In the future, the implementation of more advanced data protection technologies and the active role of all stakeholders in maintaining data security in the cloud will be very important to support the development of safer cloud technology.

BIBLIOGRAFI

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2018). Key Issues for Embracing The Cloud Computing to Adopt A Digital Transformation: A Study of Saudi Public Sector. *Procedia Computer Science*, *130*, 1037–1043.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in Cloud Computing: Opportunities and Challenges. *Information Sciences*, *305*, 357–383.

Arafat, M. (2018). Information Security Management System Challenges Within A Cloud Computing Environment. *Proceedings of The 2nd International Conference On Future Networks And Distributed Systems*, 1–6.

Dunggio, N., & Fuad, A. M. (2023). Perlindungan Data Pribadi Cloud Computing System (Google Drive) Ditinjau dari Perspektif Undang Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. *Sultan Amai Staatsrecht Journal*, *1*(01), 21–38.

George, A. S., George, A. S. H., & Baskar, T. (2023). Edge Computing and The Future of Cloud Computing: A Survey of Industry Perspectives And Predictions. *Partners Universal International Research Journal*, *2*(2), 19–44.

Hasanah, U., & Dinalestari Purbawati, S. E. (2024). *Digitalisasi Akuntansi: Transformasi, Teknologi Dan Tren*. Jakad Media Publishing.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The Rise Of "Big Data" On Cloud Computing: Review and Open Research Issues. *Information Systems*, *47*, 98–115.

Nasution, M. I. P. (2023). Keamanan dan Privasi Data dalam Lingkungan Cloud Computing: Tantangan dan Solusi. *Kohesi: Jurnal Sains Dan Teknologi*, *1*(10), 71–80.

Ogborigbo, J. C., Sobowale, O. S., Amienwalen, E. I., Owoade, Y., Samson, A. T., Egerson, J., Ogborigbo, J. C., Sobowale, O. S., Amienwalen, E. I., & Owoade, Y. (2024). Strategic Integration of Cyber Security in Business Intelligence Systems for Data Protection and Competitive Advantage. *World Journal Of Advanced Research And Reviews*, *23*(1), 81–96.

Oladoyinbo, T. O., Adebiyi, O. O., Ugonnia, J. C., Olaniyi, O. O., & Okunleye, O. J. (2023). Evaluating and Establishing Baseline Security Requirements in Cloud Computing: An Enterprise Risk Management Approach. *Asian Journal Of Economics, Business And Accounting*, *23*(21), 222–231.

Rachmad, Y. E., Dewantara, R., Junaidi, S., Firdaus, M., & Sulistianto, S. W. (2023). *Mastering Cloud Computing (Foundations And Applications Programming)*. PT. Sonpedia Publishing Indonesia.

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.

Sudiantini, D., Naiwasha, A., Izzati, A., & Rindiani, C. (2023). Penggunaan Teknologi pada Manajemen Sumber Daya Manusia di dalam Era Digital Sekarang. *Digital Bisnis: Jurnal Publikasi Ilmu Manajemen Dan E-Commerce*, *2*(2), 262–269.

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy In Cloud Computing. *International Journal of Distributed Sensor Networks*, *10*(7), 190903.

Sunyaev, A., & Sunyaev, A. (2020). Cloud Computing. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, 195–236.

Ula, M. (2019). Analisis Metode Pengamanan Data pada Layanan Cloud Computing. *TECHSI-Jurnal Teknik Informatika*, *11*(1), 125–138.

Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *Ieee Access*, *8*, 131723–131740.

Younis, Y. A., Kifayat, K., & Merabti, M. (2014). An Access Control Model For Cloud Computing. *Journal of Information Security and Applications*, *19*(1), 45–60.