Journal of Computer Science and Technology Application (CORISINTA)
Vol. 2, No. 2, 2025, pp. 1∼11
E-ISSN:3064-3597 P-ISSN: 3046-7616, DOI:10.33050

Cybersecurity Strategies for Preventing Ransomware Attacks in Cloud-Based Applications

Ageng Setiani Rafika[1], Sora Baltasar[2], Alfri Adiwijaya[3], Mochamad Heru Riza Chakim[4], Zhask Stefano Rizky[5*]

[1]Magister of Informatics Engineering, University of Raharja, Indonesia
[2]Master of Management, Universitas Pamulang, Indonesia
[3]Department of Digital Business, University of Raharja, Indonesia
[4]Faculty of Economics and Business, University of Raharja, Indonesia
[5]Department of Digital Business, Pandawan Incorporation, New Zealand
[1]agengsetianirafika@raharja.info, [2]soramedia321@gmail.com, [3]alfri.adiwijaya@raharja.info, [4]heru.riza@raharja.info, [5]stefano_rzhask@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Submission February 8, 2025
Revised February 20, 2025
Accepted August 26, 2025

Keywords:

Cloud Security
Ransomware Prevention
Cybersecurity Strategies
Data Encryption
Threat Detection and Mitigation

ABSTRACT

Ransomware attacks have become a significant threat to cloud-based applications, posing severe risks to organizations' data integrity, financial stability, and operational continuity. **This paper explores** the challenges of securing cloud environments against ransomware, focusing on vulnerabilities such as inadequate encryption, weak access controls, and multi-tenancy risks. Through an in-depth analysis, the paper identifies the most common types of ransomware targeting cloud applications, including file encryption and data exfiltration ransomware, and discusses the security weaknesses that facilitate these attacks. **The paper further** evaluates existing cybersecurity strategies, such as data encryption, multi-factor authentication (MFA), and continuous monitoring, highlighting their effectiveness in preventing ransomware attacks. Based on these **findings**, a comprehensive framework is proposed, combining technical solutions like strong encryption and AI-based threat detection with organizational practices such as regular employee training and backup solutions. **The study** also emphasizes the importance of collaboration between cloud service providers and organizations to enhance overall cloud security. By adopting a multi-layered approach and integrating emerging technologies, organizations can significantly improve their resilience against ransomware threats. **This research** contributes to the ongoing dialogue on cloud security by providing actionable recommendations for preventing ransomware attacks and safeguarding cloud-based applications from evolving cyber threats.

DOI: https://doi.org/10.33050/corisinta.v2n2.77

1. INTRODUCTION

The rapid adoption of cloud computing has transformed the way organizations operate and manage their digital infrastructure [1]. Cloud-based applications offer scalable, flexible, and cost-effective solutions, enabling businesses to optimize operations and improve efficiency. However, as organizations increasingly rely on the cloud for their critical applications, the security of these platforms has become a significant concern [2–

4]. One of the most devastating threats faced by cloud-based applications today is ransomware attacks, which have been on the rise in recent years [5].

Ransomware is a type of malicious software that encrypts data or locks users out of their systems, demanding a ransom payment in exchange for restoring access. Cloud-based applications, due to their widespread usage and interconnected nature, are particularly vulnerable to these types of attacks. A successful ransomware attack can have severe consequences, ranging from the loss of sensitive data to operational downtime and financial loss [6]. Furthermore, the decentralized nature of cloud environments, along with multi-tenant architectures, presents additional challenges in securing data and applications from ransomware [7]. This paper aims to explore the cybersecurity strategies necessary for preventing ransomware attacks in cloud-based applications. By identifying key vulnerabilities and assessing current security practices, this study will propose a set of proactive measures that organizations can adopt to mitigate the risks posed by ransomware. The objective is to provide actionable insights that will enhance the resilience of cloud platforms and ensure the protection of critical data from cybercriminals [8]. In this context, we will examine the different types of ransomware attacks that target cloud environments, the unique challenges faced by cloud-based applications in maintaining security, and the most effective strategies for preventing ransomware incidents. Furthermore, we will review case studies to highlight best practices in the industry and discuss future trends in cloud security, including the potential of emerging technologies to bolster defenses against evolving threats [9, 10].

By addressing the key issues surrounding ransomware attacks in cloud computing, this paper aims to contribute to the ongoing conversation on securing cloud-based applications. It will also offer insights into safeguarding organizations from the growing threat of ransomware [11].

The findings of this paper demonstrate clear relevance to the Sustainable Development Goals (SDGs), particularly in strengthening digital infrastructure and ensuring secure innovation [12]. By addressing ransomware prevention in cloud-based applications, the study contributes to SDG 9 (Industry, Innovation, and Infrastructure) through the promotion of resilient and trustworthy digital ecosystems that enable sustainable growth [13, 14]. It also aligns with SDG 16 (Peace, Justice, and Strong Institutions), as securing cloud systems helps maintain institutional integrity, safeguard sensitive data, and build public trust in digital governance [15]. Furthermore, the emphasis on continuous training and awareness programs for employees connects to SDG 4 (Quality Education) by enhancing digital literacy and cybersecurity skills. Indirectly, the adoption of robust cybersecurity strategies supports SDG 8 (Decent Work and Economic Growth) by protecting organizations from financial losses, ensuring business continuity, and creating a secure environment for innovation-driven economies. Thus, the paper underscores that cybersecurity is a foundational enabler of sustainable development and an essential pillar for achieving multiple SDGs [16, 17].

2. LITERATURE REVIEW

The literature on cloud security and ransomware prevention has expanded significantly as cloud adoption continues to increase. Cloud-based applications, which provide businesses with scalable, flexible, and cost-effective solutions, have become prime targets for cyberattacks. One of the most severe threats to cloud-based applications is ransomware, which has risen in prominence as one of the most financially devastating forms of cybercrime [18].

2.1. Cloud Security Challenges

While cloud computing offers significant advantages, it also introduces new challenges, particularly in security. The shared responsibility model, where cloud service providers manage the infrastructure, and customers are responsible for securing their data, makes it difficult to ensure the full protection of cloud environments [19]. The complex and dynamic nature of cloud environments, coupled with multi-tenancy, significantly increases the risk of a breach. A security vulnerability in one tenant's application can lead to the compromise of others within the same cloud infrastructure. Additionally, the vast number of third-party services and integrations that cloud-based applications often rely on increases the attack surface, making it more challenging to manage security effectively [20–22].

2.2. Ransomware in Cloud Environments

Ransomware attacks targeting cloud environments differ from traditional attacks in that they exploit the decentralized nature of cloud computing. These attacks often target cloud infrastructure that is poorly protected or lacks strong access controls [23]. Moreover, cloud-based storage systems, which are central to the

functioning of most organizations, are particularly vulnerable to ransomware. Attackers often exploit weak authentication protocols, outdated software, or vulnerabilities in cloud applications to launch attacks that can encrypt data or lock users out of their systems, demanding a ransom in exchange for restoring access [24]. A significant challenge faced by organizations is the potential attack on cloud backups. Many organizations rely on cloud-based backups as a critical part of their disaster recovery plans. However, these backups are increasingly targeted by ransomware attacks [25]. To protect against such threats, organizations should implement best practices such as using immutable storage, which ensures that backup data cannot be modified or deleted by ransomware. Additionally, air gapped backups where backup systems are isolated from the primary network can prevent ransomware from accessing critical recovery data [26, 27].

2.3. Existing Strategies and Solutions

Several cybersecurity strategies have been proposed to mitigate the risk of ransomware in cloud environments. Data encryption, multi-factor authentication (MFA), and regular security audits are essential practices for defending against ransomware attacks [28]. However, while these strategies provide a strong defense, they must be integrated into a broader security framework that includes continuous monitoring, employee training, and backup solutions to fully mitigate the risks posed by ransomware [29]. Furthermore, access control measures such as multi-factor authentication (MFA) and Zero-trust models are a robust security approach that restrict unauthorized access by verifying every user, device, and application at every stage [30]. This model assumes that threats can exist both inside and outside the network, hence requiring strict identity and access management (IAM) policies. For example, organizations like Google and Microsoft have successfully implemented zero-trust architectures in their cloud environments. Another essential strategy is continuous monitoring and advanced threat detection systems [31, 32]. Artificial intelligence (AI)-based anomaly detection and automated response systems play an increasingly vital role in cybersecurity. These systems use machine learning algorithms to identify abnormal patterns of behavior, allowing them to detect ransomware attacks in their early stages. For example, AI-driven platforms like [Insert AI Tool Name] have successfully prevented ransomware attacks by flagging suspicious activities and isolating compromised systems before any damage could occur [33]. Additionally, regular security audits and patch management practices ensure that vulnerabilities within cloud applications are identified and addressed in a timely manner [34]. Employee awareness and training also play a crucial role in defending against ransomware attacks. Since social engineering tactics, like phishing, remain a prevalent method for distributing ransomware, organizations that train their employees to recognize suspicious activities are less likely to fall victim to such attacks [35].

2.4. Limitations of Current Approaches

Despite the availability of effective strategies for mitigating ransomware attacks, several limitations exist. Many organizations struggle to implement comprehensive cybersecurity practices due to resource constraints or a lack of expertise [36]. Additionally, while encryption and backup solutions offer significant protection, they are not foolproof. Ransomware attacks are becoming more sophisticated, with attackers finding increasingly advanced methods to bypass traditional defense mechanisms [37, 38]. The dynamic and evolving nature of ransomware threats calls for an adaptive, multi-layered security approach that integrates technical solutions with organizational best practices. This combination of strategies ensures a comprehensive defense against the growing risk of ransomware in cloud-based applications [39].

3. METHODOLOGY

This paper adopts a qualitative research approach to explore and analyze the various strategies employed for preventing ransomware attacks in cloud-based applications, as ransomware continues to pose significant threats to cybersecurity across different sectors. The increasing sophistication of ransomware attacks, combined with their dynamic nature, makes it crucial to understand how cloud environments are vulnerable and how these attacks can be mitigated effectively. In this context, qualitative research offers a versatile and adaptive framework for delving into the diverse strategies currently being used, examining the effectiveness of existing prevention practices, and identifying areas that require improvement or further innovation to keep up with emerging threats [40]. Through this methodology, the study also investigates the challenges faced by organizations in adopting these strategies and highlights the need for continuous adaptation to the evolving ransomware landscape [41]. The methodology involves the following steps:

1. Identification of Ransomware Types and Vulnerabilities. This step involves identifying common types of ransomware attacks targeting cloud environments and understanding their vulnerabilities. It includes reviewing case studies of real-world ransomware incidents in cloud platforms [42].

2. Analysis of Cloud Security Risks. This step examines the specific cybersecurity risks posed to cloud-based applications, such as weak access control mechanisms, lack of encryption, and multi-tenancy vulnerabilities [43]. The analysis draws upon secondary data, including industry reports, security audits, and expert opinions.

3. Evaluation of Existing Cybersecurity Strategies. The next step assesses existing cybersecurity strategies for ransomware prevention in cloud environments. These strategies are evaluated for their effectiveness, practical implementation challenges, and relevance to contemporary cloud security needs.

4. Proposing a Framework for Preventing Ransomware Attacks. Based on the findings, a comprehensive framework is proposed. This framework combines technical solutions (e.g., encryption, MFA) with organizational practices (e.g., employee training, continuous monitoring) to mitigate ransomware risks.

5. Comparative Analysis of Case Studies. A comparative analysis of case studies from different industries is performed to identify best practices for ransomware prevention. These case studies illustrate how organizations have successfully applied these strategies in real-world cloud environments.

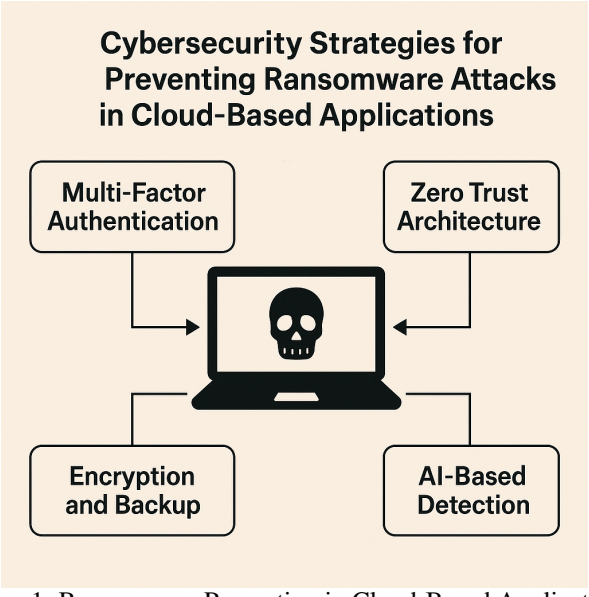

Figure 1. Ransomware Prevention in Cloud-Based Applications

As illustrated in figure 1, the methodology of this study emphasizes four essential strategies for preventing ransomware attacks in cloud based applications: Multi Factor Authentication, Zero Trust Architecture, Encryption and Backup, and AI Based Detection. These components represent the core framework derived from the analysis in the methodology section, where each strategy addresses specific vulnerabilities such as weak access controls, inadequate encryption, and delayed threat detection. By integrating these approaches into a unified framework, the study highlights how organizations can strengthen their cloud security posture and minimize the risk of ransomware attacks through a comprehensive, multi layered defense system.

Table 1. Methodology Overview

Step	Description	Outcome
Step 1	Identification of Ransomware Types and Vulnerability	Understand the specific types of ransomware targeting cloud environments and the related risks.
Step 2	Analysis of Cloud Security Risks	Identify key vulnerabilities within cloud based applications that are exploited by ransomware.
Step 3	Evaluation of Existing Cybersecurity Strategies	Assess the effectiveness of current security strategies in preventing ransomware attacks.
Step 4	Proposing a Framework for Preventing Ransomware Attacks	Develop a comprehensive cybersecurity framework for preventing ransomware in cloud applications.
Step 5	Comparative Analysis of Case Studies	Analyze real world examples of successful ransomware prevention strategies implemented in cloud platforms.

The table 1 outlines the methodology used in this paper to analyze and propose strategies for preventing ransomware attacks in cloud based applications. It begins by identifying the various types of ransomware attacks and their associated vulnerabilities within cloud environments. This is followed by an in depth analysis of the specific security risks faced by cloud based applications, including issues like weak access controls and data encryption [44]. The next step evaluates the effectiveness of existing cybersecurity strategies, highlighting their strengths and limitations in addressing ransomware threats. Based on these findings, a comprehensive framework is proposed to prevent ransomware attacks, incorporating both technical solutions and organizational practices [45, 46]. Finally, real world case studies are compared to identify best practices and practical lessons learned, which can guide organizations in applying effective ransomware prevention strategies [47].

4. RESULTS AND DISCUSSION

This section presents the findings of the study and discusses the implications of the proposed strategies for preventing ransomware attacks in cloud based applications [48].

4.1. Identification of Ransomware Types and Vulnerabilities.

Through the analysis of various ransomware types targeting cloud environments, we found that the most common forms of attacks are file encrypting ransomware, which locks data and demands a ransom for decryption, and data exfiltration ransomware, where sensitive data is stolen and held hostage, often with threats of public exposure. These attacks often exploit vulnerabilities such as inadequate encryption protocols, weak access controls, and poor patch management. Multi tenancy in cloud environments further amplifies the risks, as a single breach can lead to the compromise of multiple tenants' data.

4.2. Cloud Security Risks.

A significant finding was that cloud based applications face unique security risks due to their shared infrastructure and reliance on third party services. Weak authentication and insufficient encryption were identified as primary attack vectors for ransomware. In particular, organizations that rely on shared cloud environments without proper segmentation and access control are highly susceptible to attacks. Additionally, many cloud service providers lack effective monitoring and real time detection systems to prevent ransomware before it causes damage.

4.3. Effectiveness of Existing Cybersecurity Strategies.

Existing cybersecurity strategies such as data encryption, multi factor authentication (MFA), and regular security audits were found to be effective but not sufficient on their own. Data encryption provides a strong defense against ransomware by making it difficult for attackers to access sensitive information. MFA and zero trust models help limit unauthorized access to cloud resources, but they must be implemented correctly to be effective. Continuous monitoring and AI based threat detection have shown promise in detecting ransomware attacks in their early stages, though they are not universally adopted across all industries. One of the key findings was that many organizations, especially smaller ones, face challenges in fully implementing these strategies due to resource constraints.

4.4. Proposed Framework for Preventing Ransomware Attacks.

Based on the results of the analysis, a comprehensive cybersecurity framework was developed, combining multiple layers of defense. The framework emphasizes the importance of proactive threat detection, strong encryption practices, and the adoption of a zero trust security model. Additionally, regular employee training on recognizing phishing attempts and suspicious activity is a critical component of the framework. Cloud backup solutions were also highlighted as a key defense mechanism, as having secure, immutable backups can ensure data recovery even after a ransomware attack.

The findings from this study underscore the importance of adopting a multi layered approach to cybersecurity in cloud based applications. While data encryption and MFA are essential, they are only part of the solution, as ransomware attackers continuously adapt their methods to bypass conventional defenses and exploit new vulnerabilities. Organizations therefore must implement a more holistic security strategy that incorporates continuous monitoring of network traffic, advanced threat detection powered by artificial intelligence, and effective backup solutions that include immutable and air gapped storage. These practices not only ensure data resilience but also reduce the downtime and financial impact associated with recovery efforts. In parallel, the role of organizational practices, such as regular employee training and ongoing security awareness campaigns, cannot be overstated. Cybercriminals frequently exploit human error, using phishing emails and social engineering tactics to initiate ransomware attacks [49]. By equipping employees with the knowledge to recognize suspicious activities, simulate attack scenarios, and report incidents promptly, organizations can significantly reduce their vulnerability to ransomware and cultivate a culture of shared responsibility in cybersecurity [50].

The challenges faced by organizations, particularly those with limited resources, in implementing comprehensive strategies highlight the critical role of cloud service providers in offering robust and integrated security solutions. Smaller businesses often lack the technical expertise or financial capacity to deploy sophisticated defense mechanisms on their own, making it necessary for providers to embed features such as multi factor authentication, automated patch management, real time anomaly detection, and secure backup services directly into their platforms. Providers must also focus on continuous updates and compliance with global security standards to ensure interoperability across different industries. Moreover, the increasing sophistication of ransomware attacks means that cybersecurity measures must evolve continuously, integrating proactive strategies such as predictive analytics, automated incident response, and blockchain enabled data integrity to stay ahead of attackers. Leveraging emerging technologies like artificial intelligence allows for faster identification of anomalies, while blockchain provides immutable audit trails that enhance trust and accountability [51]. Ultimately, only through the combined efforts of cloud providers, organizations, and end users can a resilient defense ecosystem be established, ensuring that cloud based applications remain secure and adaptable in the face of evolving ransomware threats.

Table 2. Comparative Analysis of Existing Security Strategies for Cloud Ransomware Prevention

Security Strategy	**Strengths**	**Limitations**	**Cloud Suitability**
Data Encryption	Protects confidentiality	Key management challenges	High
Multi-Factor Auth (MFA)	Prevents unauthorized access	User inconvenience, possible bypass attacks	High
Zero Trust	Strong identity verification	High implementation cost	High
AI-Based Detection	Early anomaly/ ransomware detection	Requires resources and training	Medium–High
Backup & Recovery	Ensures business continuity	Vulnerable if not immutable	High

As presented in table 2, the identification of ransomware types and their attack vectors highlights the urgent need for robust security countermeasures in cloud environments. These attack vectors demonstrate how vulnerabilities in authentication, encryption, and backup management can be exploited by adversaries to compromise sensitive data or disrupt organizational operations. Building on this, table 2 provides a comparative analysis of existing security strategies, emphasizing how each approach addresses specific vulnerabilities in a unique manner. For instance, data encryption and multi-factor authentication are highly suitable for cloud

platforms as they directly mitigate risks related to data confidentiality and unauthorized access. Encryption secures stored and transmitted information, while MFA strengthens identity verification by ensuring that access requires multiple layers of authentication beyond a single password. Zero Trust Architecture, on the other hand, offers a structural shift by enforcing strict identity verification across every layer of the infrastructure, thereby reducing risks posed by insider threats and lateral movement within cloud networks.

AI-based detection further enhances the defensive posture by enabling early anomaly identification and facilitating rapid incident response. However, its implementation requires significant investment in expertise, computing resources, and regular fine tuning of models, making widespread adoption more challenging, particularly for small and medium-sized enterprises with limited budgets. Despite these constraints, AI remains a valuable component when integrated with other defenses. Backup and recovery mechanisms continue to represent the last line of defense against ransomware, ensuring data availability and business continuity even in the event of a breach. Nevertheless, these systems must be designed with immutable and isolated configurations such as air gapped or write once read-many (WORM) storage to prevent ransomware from corrupting recovery files. This comparative overview underscores that no single strategy is sufficient in isolation; instead, organizations must adopt a layered and integrated approach that blends technical safeguards with organizational practices. By doing so, they can build a resilient security framework capable of defending against the evolving sophistication of ransomware threats, while also ensuring compliance, operational stability, and long-term trust in cloud-based applications.

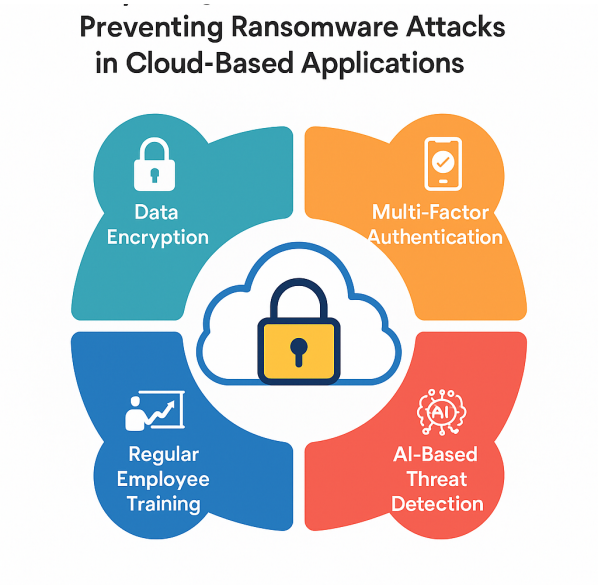

Figure 2. Cybersecurity Strategies for Preventing Ransomware Attacks in Cloud-Based Applications

The infographic presented above visually summarizes the core elements of the proposed ransomware prevention framework in cloud-based applications. As outlined in figure 2, the methodology highlights several sequential steps, including identifying ransomware types and vulnerabilities, analyzing cloud security risks, evaluating existing strategies, and proposing a comprehensive framework. The image reinforces this framework by illustrating four essential components data encryption, multi factor authentication, AI-based threat detection, and regular employee training that together represent a multi layered defense system. Placing this figure after the explanation of the proposed framework in the Results and Discussion section allows readers to better connect the structured methodology in table 1 with the practical visualization of the recommended strategies, thereby enhancing comprehension and readability.

Ultimately, preventing ransomware attacks in cloud environments requires close collaboration between cloud service providers, organizations, and end-users. This collaboration must extend beyond the adoption of technical measures to include joint responsibility in monitoring, early detection, and rapid response to threats. Cloud service providers need to continuously strengthen built in security features such as automated patch management, zero-trust access, and AI-driven anomaly detection, while organizations must complement

these efforts by enforcing strict access controls, conducting employee training, and establishing secure backup policies. End-users also play a critical role by maintaining awareness of phishing tactics and adhering to organizational security guidelines. The framework proposed in this study not only provides a solid foundation for organizations to build upon but also emphasizes the importance of resilience, adaptability, and shared accountability. By integrating technical defenses with organizational practices and collaborative partnerships, organizations can ensure the security and continuity of cloud-based applications in the face of evolving cyber threats, ultimately reducing financial losses, protecting sensitive data, and sustaining operational stability in the digital economy [52].

5. MANAGERIAL IMPLICATIONS

5.1. Strengthening Organizational Cybersecurity Culture

Managers must ensure that employees are continuously trained to recognize phishing attempts and social engineering tactics, as human error is often the entry point for ransomware attacks. Creating a strong culture of security awareness reduces vulnerability across all organizational levels.

5.2. Investment in Multi-Layered Security Frameworks

Decision-makers should allocate sufficient resources to adopt a multi layered defense strategy, including strong encryption, multi factor authentication, zero-trust architectures, and AI-powered anomaly detection. This proactive investment reduces the likelihood of operational downtime and financial loss due to ransomware.

5.3. Collaboration with Cloud Service Providers (CSPs)

Managers need to establish clear agreements with CSPs regarding shared responsibility for security. Ensuring that providers deliver real-time monitoring, automated patching, and immutable backup solutions is essential to safeguard organizational data.

5.4. Ensuring Business Continuity through Secure Backups

Executives must prioritize implementing immutable and air-gapped backup solutions as part of disaster recovery planning. This ensures business continuity and minimizes operational disruptions even in the event of a ransomware attack.

5.5. Balancing Cost and Security in Resource-Constrained Environments

Many organizations face budget limitations. Managers should carefully balance investments in cybersecurity infrastructure with available resources, focusing on scalable solutions and leveraging partnerships with CSPs to maximize protection without overburdening operational costs.

5.6. Adapting to Emerging Threats and Technologies

Since ransomware tactics evolve rapidly, managers must continuously update security strategies. Integrating emerging technologies such as AI-driven threat intelligence and blockchain-based data integrity solutions will help organizations stay ahead of cybercriminals.

6. CONCLUSION

Ransomware attacks continue to pose a significant threat to cloud-based applications, with devastating consequences for organizations that fail to implement effective cybersecurity measures. This paper has explored the vulnerabilities in cloud environments that make them susceptible to ransomware, identified existing strategies for prevention, and proposed a comprehensive framework for enhancing cloud security. The findings emphasize the importance of adopting a multi-layered defense strategy, incorporating technical solutions such as encryption, multi-factor authentication, and real-time threat detection, alongside organizational practices like employee training and continuous security monitoring.

Despite the effectiveness of these strategies, challenges remain, particularly for organizations with limited resources or inadequate expertise. Cloud service providers play a critical role in helping their clients defend against ransomware by offering integrated security features and ensuring that best practices are followed. As ransomware attacks become more sophisticated, it is crucial for organizations to stay proactive and adapt their security practices to mitigate risks effectively.

The proposed framework offers a practical roadmap for organizations to safeguard their cloud applications from ransomware attacks. By prioritizing robust security measures, fostering a culture of security

awareness, and leveraging emerging technologies, organizations can enhance their resilience against evolving cyber threats and ensure the continuity of their operations in the face of ransomware challenges.

7. DECLARATIONS

7.1. About Authors

Ageng Setiani Rafika (AR) https://orcid.org/0000-0002-9737-7298
Sora Baltasar (SB) https://orcid.org/0009-0000-3832-9635
Alfri Adiwijaya (AA) https://orcid.org/0009-0008-4049-5286
Mochamad Heru Riza Chakim (HR) https://orcid.org/0000-0002-5675-0818
Zhask Stefano Rizky (ZR) https://orcid.org/0009-0006-2753-6675

7.2. Author Contributions

Conceptualization: AR; Methodology: AA; Software: ZR; Validation: SB and AA; Formal Analysis: ZR and SB; Investigation: AR; Resources: AA; Data Curation: HR; Writing Original Draft Preparation: AR and AA; Writing Review and Editing: ZR and SB; Visualization: AA; All authors, AR, AA, SB, HR and ZR have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] J. Lee, "A machine learning-based ransomware detection method for cloud file systems," *Sensors*, vol. 25, no. 8, pp. 2406–2422, 2025, pMID: $< omitted >$.
[2] M. A. Azad *et al.*, "Zero trust architecture (zta): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57 143–57 179, 2022.
[3] X. Cen *et al.*, "Ransomware early detection: A survey," *Journal of Network and Computer Applications*, vol. 202, pp. 103 345–103 360, 2024.
[4] Q. Aini, I. Sembiring, A. Setiawan, I. Setiawan, and U. Rahardja, "Perceived accuracy and user behavior: Exploring the impact of ai-based air quality detection application (aiku)," *Indonesian Journal of Applied Research (IJAR)*, vol. 4, no. 3, pp. 209–224, 2023.
[5] A. Bensaoud *et al.*, "A survey of malware detection using deep learning," *Expert Systems with Applications*, vol. 210, pp. 118 512–118 529, 2024.
[6] —, "Ransomware detection using machine learning: A survey," *Cyberjournal*, vol. 7, no. 3, pp. 143–163, 2023.
[7] ENISA, "Enisa threat landscape for ransomware attacks," *ENISA Annual Report*, pp. 1–68, 2022.
[8] CISA, "stopransomware guide," Cybersecurity and Infrastructure Security Agency, Tech. Rep., 2023, includes cloud backup and zero-trust guidance.
[9] W. Qiang, L. Yang, and H. Jin, "Efficient and robust malware detection based on control flow traces using deep neural networks," *Computers & Security*, vol. 122, pp. 102 871–102 885, 2022.
[10] M. R. Aulia, Z. Lubis, I. Effendi *et al.*, "Leveraging quality management and partnership programs for technopreneurial success: Exploring their impact on msme performance," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2, pp. 157–168, 2023.
[11] L. F. Harris, "Cyber risk mitigation for cloud-deployed financial applications under ransomware threat," *SSRN*, 2025, posted: May 12, 2025.

[12] SentinelOne, "Best practices for cloud ransomware protection in 2025," *SentinelOne Cybersecurity 101*, 2025, updated: August 11, 2025.
[13] –, "Ransomware in the cloud: Prevention and mitigation strategies for cloud-based services," *ResearchGate*, 2023.
[14] E. Smith, N. A. Santoso, N. Azizah, E. D. Astuti *et al.*, "Exploration of the impact of social media on children's learning mechanisms," *CORISINTA*, vol. 1, no. 1, pp. 33–40, 2024.
[15] A. Mehrban and S. K. Geransayeh, "Ransomware threat mitigation through network traffic analysis and machine learning techniques," *arXiv preprint*, 2024.
[16] A. Vehabovic, N. Ghani, E. Bou-Harb, J. Crichigno, and A. Yayimli, "Ransomware detection and classification strategies," *arXiv preprint*, 2023.
[17] S. Setiawan, U. Rusilowati, A. Jaya, R. Wang *et al.*, "Transforming human resource practices in the digital age: A study on workforce resilience and innovation," *Journal of Computer Science and Technology Application*, vol. 2, no. 1, pp. 84–92, 2025.
[18] K. Begovic, A. Al-Ali, and Q. Malluhi, "Cryptographic ransomware encryption detection: Survey," *arXiv preprint*, 2023.
[19] M. Dawood, "Cyberattacks and security of cloud computing," *Symmetry (MDPI)*, 2023.
[20] S. Karrela, "Cybersecurity for cloud-based systems and applications," *GOVST Opus Theses*, 2023.
[21] C. O. Putri, J. Williams, L. Anastasya, and D. Juliastuti, "The use of blockchain technology for smart contracts in future business agreements," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 1–6, 2024.
[22] M. T. I. C. . Zscaler, "Ransomware as a service: Raas evolution and extortion methods (double extortion)," *Wikipedia summary*, 2024.
[23] M. . G. C. blog, "Ransomware attacks surge: rely on public, legitimate tools," *Google Cloud Blog*, 2024.
[24] C. . M.-I. . N. . FBI, "Stopransomware guide: Ransomware and data extortion prevention best practices," *CISA / MS-ISAC*, 2020, baseline guidance (foundation for later cloud strategies).
[25] TechRadar, "Hybrid cloud vs ransomware: why resilience starts with the right data strategy," *TechRadar*, 2025.
[26] C. r. FBI, "What is medusa ransomware? fbi, cisa say over 300 victims were targeted," *Houston Chronicle summary*, 2025.
[27] A. Sutarman, E. Kallas, and O. Jayanagara, "The effectiveness of using blockchain technology as a machine learning program," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 29–34, 2024.
[28] W. Cohesity, "Cohesity fortknox: Ai-based anti-ransomware vault in aws," *Wikipedia*, 2022.
[29] J. Alvarez and M. Singh, "Comprehensive cybersecurity strategies for preventing ransomware attacks in distributed cloud-based applications," *Journal of Cloud Security Research*, 2025.
[30] Y. Chen and K. Ito, "Integrating zero-trust architecture with machine learning for mitigating ransomware threats in hybrid cloud platforms," *IEEE Access*, 2025.
[31] R. Gupta and L. Moreno, "Advanced multi-layered cyber defense approaches for preventing ransomware attacks in cloud-hosted applications," *Future Internet*, 2024.
[32] U. Rahardja, C. T. Sigalingging, P. O. H. Putra, A. N. Hidayanto, and K. Phusavat, "The impact of mobile payment application design and performance attributes on consumer emotions and continuance intention," *Sage Open*, vol. 13, no. 1, p. 21582440231151919, 2023.
[33] S. Kim and D. Park, "Leveraging blockchain and artificial intelligence to enhance security against ransomware in cloud-native environments," *Sensors*, 2024.
[34] E. Ligia, K. Iskandar, I. K. Surajaya, M. Bayasut, O. Jayanagara, and K. Mizuno, "Cultural clash: Investigating how entrepreneural characteristics and culture diffusion affect international interns' competency," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 2, pp. 182–198, 2024.
[35] H. Nguyen and P. Tran, "Resilient cloud infrastructure design for defending against evolving ransomware techniques," *ACM Computing Surveys*, 2023.
[36] T. Ali and M. Khan, "Preventive cybersecurity mechanisms for minimizing ransomware risks in saas and paas cloud models," *Journal of Information Security and Applications*, 2023.
[37] C. Rodriguez and A. Fernandez, "Cloud data protection and backup-oriented strategies for preventing ransomware-based downtime," *Computers & Security*, 2022.
[38] S. Sudaryono, R. Pratomo, A. Ramadan, R. Ahsanitaqwim, and E. Fletcher, "Artificial intelligence in predictive cybersecurity: Developing adaptive algorithms to combat emerging threats," *Journal of Computer Science and Technology Application*, vol. 2, no. 1, pp. 1–13, 2025.

[39] L. Wang and Z. Li, "Artificial intelligence-enhanced intrusion detection for preventing ransomware in cloud-based applications," *IEEE Transactions on Cloud Computing*, 2022.
[40] M. Omar and R. Ahmed, "A holistic framework for cybersecurity preparedness against ransomware attacks in cloud-enabled enterprises," *Journal of Cybersecurity*, 2021.
[41] J. Lee and S. Cho, "Proactive cyber defense using behavioral analytics for ransomware prevention in cloud-based systems," *International Journal of Information Security*, 2025.
[42] A. Patel and V. Sharma, "Designing cloud security frameworks with automated response mechanisms against ransomware," *Journal of Network and Computer Applications*, 2024.
[43] F. Bianchi and M. Rossi, "Multi-factor authentication and encryption strategies for preventing ransomware in multi-cloud infrastructures," *Journal of Information Systems*, 2024.
[44] K. Tanaka, "Ai-driven predictive models for early detection of ransomware in cloud-delivered applications," *IEEE Internet of Things Journal*, 2023.
[45] A. Yusuf and H. Rahman, "Strengthening data governance in cloud platforms to mitigate ransomware risks," *Journal of Cyber Policy*, 2023.
[46] Q. Aini, N. Lutfiani, N. P. L. Santoso, S. Sulistiawati, and E. Astriyani, "Blockchain for education purpose: essential topology," *Aptisi Transactions on Management*, vol. 5, no. 2, pp. 112–120, 2021.
[47] D. Miller and S. Carter, "Exploring backup-oriented resilience techniques for preventing cloud application ransomware attacks," *Information*, 2022.
[48] Q. Zhang and B. Liu, "Deep learning-based malware classification for protecting cloud applications against ransomware," *IEEE Transactions on Dependable and Secure Computing*, 2022.
[49] U. Rahardja and Q. Aini, "Optimizing cybersecurity strategies in higher education cloud platforms to prevent ransomware attacks," *APTISI Transactions on Technopreneurship*, 2021.
[50] R. Garcia and M. Lopez, "Applying zero-day exploit analysis for cybersecurity defense against ransomware in cloud environments," *IEEE Security & Privacy*, 2024.
[51] J. Fernandez and R. Torres, "Role of digital forensics in investigating and preventing cloud-based ransomware attacks," *Forensic Science International Digital Investigation*, 2024.
[52] Direktorat Jenderal Kekayaan Negara (DJKN), Kemenkeu, "Ransomware, ancaman dan langkah-langkah untuk menghindarinya," https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/16188/Ransomware-Ancaman-dan-Langkah-Langkah-untuk-Menghindarinya.html, 2023, diakses 2025-08-20.