Nusantara 1

Artikel Galleys Teknologia-Vol2.4-2101.pdf

Library - No Repository 15

Library B

Unidades Tecnológicas de Santander_DIE

Document Details

Submission ID
trn:oid:::1:3424170494

Submission Date
Nov 25, 2025, 1:32 AM GMT-5

Download Date
Nov 25, 2025, 1:33 AM GMT-5

File Name
Artikel_Galleys_Teknologia-Vol2.4-2101.pdf

File Size
627.0 KB

18 Pages

7,392 Words

45,425 Characters

10% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography

Match Groups

49 Not Cited or Quoted 8%
Matches with neither in-text citation nor quotation marks

10 Missing Quotations 2%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

7% Internet sources
5% Publications
1% Submitted works (Student Papers)

Match Groups

- **49** Not Cited or Quoted 8%
  Matches with neither in-text citation nor quotation marks
- **10** Missing Quotations 2%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

7% Internet sources
5% Publications
1% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Publication	
Doug Cairns, Roberta Amendola, Dilpreet Bajwa, Cecily Ryan, Chris Ridgard, Jared...		1%
2	Student papers	
American Public University System		<1%
3	Internet	
telsoc.org		<1%
4	Internet	
www.mdpi.com		<1%
5	Publication	
"Industry 5.0", Springer Science and Business Media LLC, 2025		<1%
6	Internet	
stax.strath.ac.uk		<1%
7	Internet	
archive.interconf.center		<1%
8	Publication	
Omowunmi F. Makinde. "chapter 7 Cloud Security for Healthcare", IGI Global, 2025		<1%
9	Internet	
nawalaeducation.com		<1%
10	Publication	
Richard Gwashy Young. "Technology, AI, and Operational Security in Banking - M...		<1%

11	Internet	
thecyberexpress.com		<1%
12	Internet	
wiki2.org		<1%
13	Internet	
eprints.umsida.ac.id		<1%
14	Internet	
www.warse.org		<1%
15	Internet	
jier.org		<1%
16	Internet	
risetpress.com		<1%
17	Internet	
www.ojsapaji.org		<1%
18	Publication	
Walt Powell. "The CISO 3.0 - A Guide to Next-Generation Cybersecurity Leadership...		<1%
19	Internet	
iieta.org		<1%
20	Internet	
international.appihi.or.id		<1%
21	Internet	
ojs.unud.ac.id		<1%
22	Internet	
studenttheses.uu.nl		<1%
23	Internet	
www.globenewswire.com		<1%
24	Internet	
core.ac.uk		<1%

25	Internet	
www.adjuris.ro		<1%
26	Internet	
epub.uni-regensburg.de		<1%
27	Internet	
gjeta.com		<1%
28	Internet	
ijbemr.com		<1%
29	Internet	
ijcopi.org		<1%
30	Internet	
ijerd.com		<1%
31	Internet	
journal.sttsimpson.ac.id		<1%
32	Internet	
majmuah.com		<1%
33	Internet	
ouci.dntb.gov.ua		<1%
34	Internet	
redc.revistas-csic.com		<1%
35	Internet	
su.diva-portal.org		<1%
36	Internet	
www.ijnrd.org		<1%
37	Internet	
yigkx.org.cn		<1%
38	Publication	
Kok Boon Oh, Giang Hoang, John Sturdy, Sarah Shuaiqi Guo. "Cybersecurity Gover...		<1%

39 Publication

Marija Zajeganović, Milan Pavlović, Milan Milivojević. "Managing Cloud Security", ... <1%

Technologia Journal: Jurnal Informatika
E-ISSN : 3046-9163
Vol.2.No.4, November 2025
DOI : https://doi.org/10.62872/xe3zrt53

Information Security in The Cloud Era: Strategies and Implementation

Nyoman Gunantara
Universitas Udayana
e-mail: gunantara@unud.ac.id

Inputed : October 09, 2025 *Revised : November 07, 2025*
Accepted : October 19, 2025 *Published : November 25, 2025*

ABSTRACT

Cloud computing has become a fundamental driver of global digital transformation, providing organizations with scalability, operational efficiency, and flexibility. However, the migration to cloud environments has also intensified cybersecurity challenges, including data breaches, misconfigurations, identity compromise, and evolving cyber-threats. This systematic literature review analyzes strategic and implementation approaches to cloud information security across multiple sectors. The study applies a structured methodology aligned with academic SLR standards to identify key security practices, technological controls, and governance frameworks. Findings reveal that effective cloud security requires a holistic model integrating Zero Trust Architecture, encryption, identity and access management, artificial intelligence-driven threat monitoring, and compliance with regulatory frameworks. Organizational readiness, human capability, and governance maturity significantly influence implementation outcomes. The study concludes that adaptive, multi-layer security models combined with continuous workforce development and regulatory harmonization are critical for building sustainable cloud resilience.

Keywords: *cloud security, cybersecurity, digital governance, zero trust.*

INTRODUCTION

The development of cloud computing technology has become the main foundation of global digital transformation, enabling organizations to improve flexibility, scalability, and operational efficiency through internet-based on-demand services. Around 94% of companies worldwide have adopted cloud technology in various forms, with a significant increase in hybrid and multi-cloud models (Baladari, 2024). Internationally, spending on public cloud services is projected to reach USD 987.7 billion by 2027, up from USD 490.3 billion in 2022 (MarketsandMarkets Research Pvt. Ltd., 2023). This growth reflects a strategic shift by organizations toward dynamic service-based infrastructure models to improve business resilience and digital innovation. On the other hand, increased cloud usage also brings new challenges in the field of information security, particularly related to data privacy, access management, and network-based threats (Alghofaili et al., 2021).

Despite the rapid adoption of cloud, cybersecurity threats to cloud infrastructure have shown a significant increase. Data from Check Point Software Technologies Ltd, (2025) notes that cyberattacks on cloud environments increased by 48% globally compared to the previous year, with a primary focus on ransomware attacks, API-based malware, and system configuration vulnerability exploits. Additionally, the Verizon Data Breach Investigations Report (2023) reveals that 19% of data breach incidents involve public cloud environments, indicating that transitioning to the cloud does not automatically guarantee improved security. Factors such as configuration errors, weak access policies, and the inability to comprehensively monitor user activity are the dominant causes of security breaches (Hughes-Lartey et al., 2021). These findings confirm that cloud security is a strategic issue that requires serious attention.

In the Asian region, including Indonesia, the adoption of cloud technology has also accelerated rapidly. A report by International Data Corporation (IDC) Asia Pacific (2022) shows that cloud adoption in Southeast Asia has increased by up to 40% in the financial, education, and government sectors. In Indonesia alone, cloud usage grew by 31.5% in 2023, driven by the government through its national digital transformation acceleration program (Indonesian Ministry of Communication and Information Technology, 2023). However, increased cloud adoption is also accompanied by increased digital security risks. The National Cyber and Crypto Agency (BSSN) reported 361 million cyberattacks throughout 2023, mostly targeting financial institutions and the public sector, with attack techniques such as brute force, DDoS, and data exfiltration (Rusydi, 2025). This shows that threats to national digital infrastructure, including cloud-based systems, are becoming more complex and have the potential to compromise the security of sensitive information.

Emerging cloud security challenges are not only technical in nature, but also include regulatory and data governance aspects. For example, issues of compliance with the General Data Protection Regulation (GDPR) in the European Union and the obligation to store data locally in accordance with Indonesian Government Regulation No. 71 of 2019 create complexity in the implementation of cross-border cloud security strategies (Budiardjo et al., 2019). Organizations are required to ensure data integrity, availability, and confidentiality, but they must also comply with provisions related to privacy and data sovereignty. Another challenge is the limited cybersecurity competence in many organizations, particularly in managing user access and digital identities in cloud systems (Rawal et al., 2023). Human error remains the biggest source of cloud security risk, with 82% of breaches involving human elements (El-Bably, 2021).

In addition to external risks, the cloud operating model itself poses new challenges related to the distribution of responsibilities between cloud service providers and customers. The shared responsibility model concept emphasizes that cloud providers are only responsible for infrastructure security, while user

organizations are responsible for their own configuration, access, and data protection (Chauhan & Shiaeles, 2023). However, many organizations still do not fully understand this role, leading to misconceptions that result in negligence in the implementation of security controls (Stewart, 2023). For example, a report by Palo Alto Networks noted that 70% of companies that experienced cloud breaches stated that internal configuration failures were a major factor (Mortimer, n.d.). This case shows that the success of a cloud security strategy depends not only on technology but also on a deep understanding of the correct security management model.

One important aspect of cloud security is the implementation of encryption technology and multi-factor authentication mechanisms to protect access to sensitive data. A study conducted by Kumar et al., (2025) shows that the use of end-to-end encryption in a cloud environment can reduce the risk of data leaks by up to 67%, while multi-factor authentication has been proven to significantly reduce the risk of illegal access. However, the implementation of cryptography-based security methods still faces obstacles in the small and medium-sized enterprise (SME) sector, particularly in terms of cost, limited IT resources, and a lack of technical knowledge (Husriadi et al., 2024). This situation explains the digital divide between large and small organizations in the safe use of cloud technology, thereby affecting the overall efficiency of cloud service usage.

On the other hand, security approaches based on Artificial Intelligence (AI) and machine learning are increasingly relevant in detecting anomalies and sophisticated threats in cloud environments. Assert that AI-based security systems are capable of detecting zero-day threats up to 30% faster than traditional systems (Eleweke et al., 2025). However, AI technology can also be exploited by malicious parties to create more complex attacks, such as automated phishing and adaptive malware (Kadbe et al., 2025). This creates a security paradox, where technology intended for protection can also become a more powerful tool for attack. Therefore, a holistic and adaptive security strategy is needed that takes into account technological developments from both the defensive and offensive sides.

The implementation of cloud security strategies requires a multi-dimensional approach that includes policies, technology, and comprehensive risk management. The concept of Zero Trust Architecture (ZTA) has become a widely developed paradigm in modern cloud security. ZTA assumes that no entity, whether internal or external, is automatically trusted, so access must be continuously validated based on strict verification and least privilege principles (Syed et al., 2022). The implementation of ZTA has been proven to increase system resilience against lateral movement attacks and credential compromise in hybrid cloud environments. A study by Smita Verma, (2025) shows that organizations implementing ZTA experience a 41% reduction in access breach incidents. However, challenges in implementing ZTA include the cost of

architecture migration, the complexity of integration with legacy systems, and the need to improve internal IT security literacy.

Another aspect that is the focus of cloud security is the organization's dependence on cloud service vendors or third-party risk. This dependence creates new exposure to the risk of cyber-attacks on the supply chain, which is increasing globally. According to a study by (Rasner, 2021), digital supply chain attacks have increased by 300% in the last five years, with many cases related to intrusions into third-party systems that then affect end users. In the context of the cloud, vendor service failures or compromises can have systemic impacts on the public sector and critical industries. Therefore, vendor risk evaluation, compliance audits, and continuous security monitoring mechanisms are essential elements of modern cloud security strategies (Richard Arogundade, 2023).

This shows that the success of cloud security depends not only on internal technology, but also on the integrity of the connected external ecosystem. The centrality of identity and access management (IAM) policies is also a major concern in the cloud ecosystem. IAM serves to regulate who can access information resources, when, and in what context.

A study by Arumugam, (2025) shows that 63% of cloud breaches stem from IAM configuration errors, including the use of default credentials, weak authentication, and excessive user access. Therefore, the implementation of IAM based on the principle of least privilege, privilege access management (PAM), and credential rotation is a requirement that cannot be ignored. This strategy needs to be supported by security training policies for employees, given that human factors remain a dominant variable in cloud data breach incidents (Ang'udi, 2023). Thus, cloud security must be understood as a system that encompasses a combination of technology, governance, and human competence.

In addition to IAM, security audits and compliance automation are important components to ensure the alignment of cloud operations with the regulatory framework. At the global level, various security standards such as ISO/IEC 27001, SOC 2, and NIST SP 800-53 are often used as references in setting cloud security policies. In Indonesia, electronic system security standards refer to BSSN Regulation No. 8 of 2020, which establishes electronic system security categories based on data criticality levels. Research by Kaur et al., (2023) confirms that the implementation of standards-based cloud audits increases the accuracy of configuration anomaly detection by 36% and speeds up security response by up to 28%. However, the adoption of compliance automation is still relatively low in the Indonesian public sector, especially in regional institutions that face technical and budgetary constraints.

Cloud-based digital transformation also affects critical sectors such as health, finance, and education. The use of cloud in the healthcare sector, for example, accelerates access to medical information, telemedicine, and health big data processing. However, these services carry the risk of sensitive patient

data leaks. Found that 23% of attacks on global healthcare facilities were related to the cloud environment, indicating the need for strict encryption and data segregation. Meanwhile, in the financial sector, the Financial Services Information Sharing and Analysis Center (FS-ISAC) reported that cloud-targeted attacks on banks and fintech companies increased by 54% in 2022, driving the need to strengthen real-time threat detection systems and integrate AI-based anti-fraud technology (Faisal et al., 2024). A similar situation occurred in the education sector, where the increased use of cloud learning platforms after the pandemic presented threats of ransomware and academic data leaks (Sam et al., 2023). Thus, the urgency of cross-sector cloud security is universal and pressing.

On the research side, academic attention to cloud security has increased significantly in the last decade. The main focus of research includes homomorphic encryption, AI-based intrusion detection, and dynamic access management. However, the literature shows that there are still research gaps related to strategies for aligning cloud security technologies with implementation practices at the organizational level and operational governance policies. In addition, research shows that the implementation of cloud security strategies in developing countries still faces different challenges compared to developed countries, such as infrastructure limitations, governance maturity, and human resource capability gaps (Adeusi et al., 2024). Therefore, an approach that comprehensively assesses the feasibility and implementation of cloud security strategies is an important contribution to the development of information security science and practice.

In the context of academic study development, a number of previous studies have contributed to the understanding of cloud-based information security, but there is still important research space to be explored further. For example, research by Khan et al., (2021) entitled Cloud Security Challenges and Opportunities in Hybrid Environments focuses on the technical challenges of hybrid architecture, but does not adequately review how organizational readiness especially in developing countries affects the effectiveness of cloud security strategy implementation. Similarly, a study by (Bishukarma, 2023) emphasizes the contribution of Zero Trust Architecture in strengthening cloud security, but does not consider implementation barriers related to human resource limitations, internal governance, and organizational operational policy readiness. Meanwhile, the research by Gupta et al., (2025) in the article provides an in-depth perspective on cloud risks in the healthcare sector, but has not developed a cross-sector approach to understand the dynamics of cloud security in the government, finance, and education sectors, which have different risk characteristics.

This research gap indicates the need for more comprehensive studies on cloud security strategies that cover not only technical dimensions but also governance, human resource readiness, and the national regulatory context. Therefore, this study offers novelty through a holistic approach that combines a

technology-based security framework, organizational policies, digital capability maturity, and regulatory dynamics in the cloud security ecosystem in Indonesia. The approach used not only assesses the effectiveness of technical mechanisms such as Zero Trust, IAM, or encryption, but also evaluates organizational readiness in terms of security awareness, human resource competencies, and legal compliance alignment. By considering multi-sector and developing country conditions, this study provides a contextual perspective that has not been widely addressed in previous literature.

In line with this focus, the main objective of this study is to evaluate information security strategies in the cloud environment and analyze their implementation in various organizational sectors in Indonesia. The results of the analysis are expected to produce a strategic framework of recommendations that is adaptive, measurable, and contextual to the development of digital threats, regulatory demands, and national organizational capacity. Thus, this study contributes to the strengthening of cloud security policies that are not only responsive to technological risks but also oriented towards the development of sustainable information security institutional capabilities.

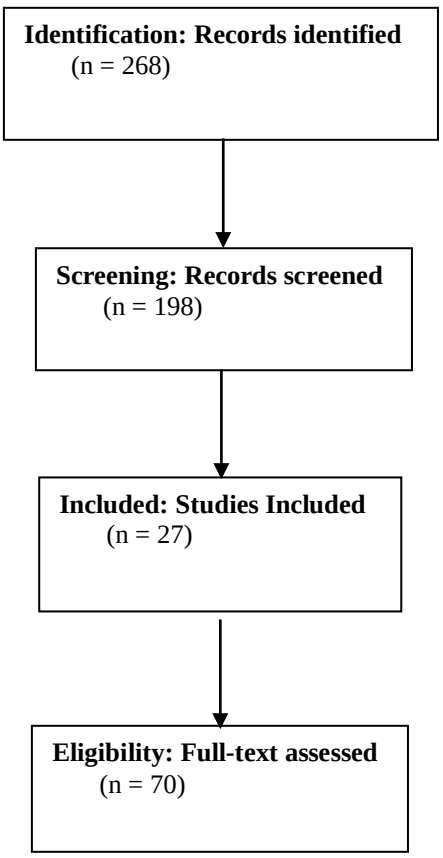
METHODOLOGY

This study uses a systematic literature review (SLR) approach to identify, evaluate, and synthesize scientific findings related to information security strategies and implementation in the cloud environment. The SLR approach was chosen because it is capable of producing comprehensive knowledge through a systematic and transparent literature selection process, thereby providing a strong empirical basis for understanding cloud security models across various industry sectors and governance (Santos et al., 2024). This methodology is also relevant in the context of information technology research because it allows researchers to evaluate cloud security practices from cross-country studies, various technology models, and different organizational contexts. The scope of the research covers scientific publications published in the last ten years (2014–2024) to capture the rapidly evolving dynamics of cloud security, both in technical dimensions such as Zero Trust, encryption, and AI-based threat detection, as well as non-technical aspects such as policy, risk management, and organizational security governance.

Data collection was conducted through the scientific databases Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar, using keywords such as cloud security, information security strategy, Zero Trust cloud, AI threat detection cloud, and cloud governance security. Articles were selected based on the following inclusion criteria: (1) reputable journal articles indexed by Scopus or WoS, (2) published between 2014 and 2024, (3) discussing cloud security strategies or cloud security implementation at the organizational level, and (4) available in English or Indonesian. Articles that focused on purely technical aspects without an organizational strategy perspective, non-peer-reviewed conference articles, and publications that did not have full access

were excluded from the analysis. This approach is in line with the procedural recommendations of Kitchenham et al. (2020) in computational research to ensure methodological validity and content relevance in scientific studies of cloud security.

The data analysis stage was conducted through a thematic coding process to identify strategic patterns covering (1) key technical approaches to cloud security, (2) cloud security governance and policy strategies, (3) human resource factors and organizational capabilities in cloud security, and (4) implementation challenges and opportunities in the context of developing countries. This process followed the framework of Braun and Clarke (2021) in thematic analysis to ensure that the interpretation of the study findings was systematic, structured, and replicable. In addition, a triangulation of sources process is carried out to verify the consistency of findings from various sectors and geographical regions, thereby strengthening the objectivity of the conclusions. The final output is a comprehensive and contextual synthesis of a cloud security strategy model to support the development of adaptive information security policies in Indonesia.



RESULTS AND DISCUSSION

Strategic Approaches to Cloud Information Security

Efforts to strengthen information security in the cloud environment require a strategic approach that encompasses the dimensions of technology,

policy, and integrated risk management. Changes in the technological landscape require organizations to develop proactive, adaptive, and intelligence-based defense mechanisms to deal with increasingly complex cyber threats. A study by (Abdulsalam & Hedabou, 2021) confirms that cloud computing increases the risk of attacks on sensitive data, so security strategies must include access management, data encryption, and continuous monitoring. From a business continuity perspective, the implementation of appropriate strategies plays an important role in maintaining data integrity while supporting the sustainability of digital business operations. In general, research shows that organizations that adopt structured cloud security strategies experience a 35% reduction in attack risk compared to those without formal security plans (Ahmadi, 2024).

The Zero Trust Architecture (ZTA) approach is one of the important foundations of modern cloud security management. This concept removes the assumption of automatic trust and implements strict validation of every access request. Rose et al. (2020) emphasize that ZTA is able to minimize the threat of lateral movement by requiring layered authentication and authorization for each user identity. The implementation of the least privilege principle in ZTA has also been proven to reduce the risk of access escalation, which is often the entry point for internal cyberattacks. Kumar and Ghrera (2022) show that the adoption of Zero Trust has reduced unauthorized access incidents by up to 41% in technology companies that rely on it. However, the successful implementation of ZTA depends on the digital readiness of the organization, including the ability to integrate security devices, the competence of technical human resources, and the readiness of internal company policies.

Another important aspect is data encryption, both when data is stored and when it is transmitted. Advanced encryption such as homomorphic encryption provides advantages in maintaining data privacy during processing without having to open the data content (Hamza et al., 2022). In the healthcare sector, data encryption has been proven to reduce the potential exposure of patient information when cloud system breaches occur (Vashishth et al., 2025). However, challenges arise in the SME sector, which faces difficulties in adopting advanced encryption algorithms due to cost and technical infrastructure limitations (Rawindaran et al., 2021). This indicates the need for a tiered-security adoption approach that accommodates differences in organizational scale so that cloud-based digital transformation remains inclusive and secure.

Meanwhile, Identity and Access Management (IAM) serves as the primary control layer in securing cloud resources. Structured IAM enables organizations to implement access restrictions based on user roles and context. 63% of cloud breaches stem from IAM configuration errors, reflecting the urgency of strengthening access policies and periodic audits of user privileges. The Privileged Access Management (PAM) approach is increasingly important to ensure that privileged access is only used as needed for operational purposes. Supports that security awareness training for employees significantly

improves the effectiveness of IAM, reducing the risk of user errors that are often the main cause of data breaches.

On the other hand, AI-driven security monitoring is an important component in supporting real-time threat detection capabilities. Machine learning-based systems have proven to be capable of identifying anomaly patterns, bot attacks, and new malware much faster than traditional mechanisms. AI-based threat detection can increase response speed by up to 30%, which is crucial in preventing attack escalation. However, the use of AI also presents the risk of technology misuse by cyber threat actors. Hackers are now utilizing AI to automate phishing attacks and generate more adaptive malware payloads. Therefore, the integration of AI in cloud security must be accompanied by algorithm transparency policies and strict control mechanisms over security system training data (Pandya, 2025).

Another major challenge relates to dependence on cloud vendors. Digital supply chain attacks have increased rapidly in recent years. Noted a 300% increase in supply chain attacks over the past five years, indicating that threats originate not only from internal vulnerabilities but also from external service providers. Vendor risk mitigation strategies include evaluating cloud providers' compliance commitments to global security standards such as ISO/IEC 27001 and conducting regular audits of cloud systems to ensure security controls are in place. Automated security audits can reduce configuration weaknesses by up to 36%, supporting the importance of a proactive approach to cloud security.

Overall, an effective strategic approach to cloud security includes a combination of technology, policy governance, risk management, and human resource competency enhancement. This combination ensures that security measures are not only technical but also integrated into the organizational culture. This comprehensive security structure not only increases resilience to attacks but also enhances stakeholder and user confidence in cloud-based digital services (Ahmad et al., 2021).

Organizational Governance, Regulatory Compliance, and Human Factor

Cloud security is not only a matter of technology, but also a matter of governance, regulation, and human competence. Governance elements determine an organization's success in implementing risk-oriented security policies. Compliance issues are crucial, given that the cloud often involves cross-border data exchange, which is subject to various global privacy regulations. Compliance with the GDPR and PP 71/2019 regarding the implementation of electronic systems is a challenge for Indonesian organizations in managing data in the global cloud. Regulatory compliance is not only a legal issue, but also affects public reputation and trust. Companies that do not implement a compliance framework tend to experience the risk of losing customers when data incidents occur.

Cloud governance challenges become even more complex in multi-cloud and hybrid cloud models. (Oladosu et al., 2021) show that organizations operating hybrid cloud models face challenges in security control consistency,

responsibility coordination, and threat visibility. The shared responsibility model is still often misunderstood by cloud users, with some organizations assuming that cloud providers are fully responsible for data security. In reality, cloud providers only secure the infrastructure, while users are responsible for access control, configuration, and data protection. This misunderstanding causes many organizations to fail to implement adequate protection at the application and internal data layers.

Amidst governance challenges, the digital security literacy of human resources is a determining factor in the successful implementation of cloud security. IBM Security (2023) notes that 82% of data breaches involve human elements. A lack of understanding of IAM principles, encryption, and basic security practices increases the likelihood of configuration errors and data leaks. Internal cybersecurity education is a fundamental necessity. Regular security training and simulation programs can increase incident response accuracy by up to 29% and reduce user errors related to credentials by up to 40%. Therefore, strengthening human resource capabilities through cybersecurity training is no longer optional, but rather a strategic priority for organizations.

In addition, organizational culture also plays an important role in supporting cloud security governance. Organizations with a strong security culture tend to be more disciplined in following security standard procedures and internal audit protocols. Katuk et al., (2024) noted that educational institutions that implement a culture of digital awareness are more successful in preventing ransomware attacks on cloud learning platforms. The involvement of top management in security policies is an important factor for success. Weak governance in the form of a lack of commitment from top management can lead to weak implementation of security controls, resulting in significant operational risks (Yusif & Hafeez-Baig, 2021).

National and international regulations are also an important framework in promoting consistent cloud security standards. In Indonesia, BSSN issued Regulation No. 8/2020 concerning electronic system security standards, which provides guidance on security controls based on data risk levels. Organizations that follow local regulatory standards have a better level of security readiness than organizations that do not have a compliance orientation. In addition, compliance automation plays a significant role in accelerating the security audit process. However, its adoption is still low in medium-sized public institutions due to limitations in IT infrastructure and budget.

Table 1. Key Governance and Compliance Components in Cloud Security

Aspect	Description	Studies
Data Sovereignty	Ensuring data is stored and processed within legal jurisdiction	(Karagiannis & Vergidis, 2021)
Policy Enforcement	Internal governance mechanisms for access control and data	(Abbas et al., 2024)

	handling	
Compliance Automation	Automated auditing and regulation monitoring tools	(Odetunde et al., 2022)
Shared Responsibility Model	Distribution of security responsibilities between CSP and client	(Singh & Sharma, 2021)

Human factors, governance maturity, and regulatory readiness form a robust cloud security ecosystem. Without a strong governance foundation, investments in advanced security technologies will not be effective in preventing cyber incident risks (Adejumo & Ogburie, 2025). This means that the successful implementation of cloud security strategies depends not only on technology, but also on the synergy of policies, human resource awareness, and regulatory infrastructure.

Implementation Outcomes, Cross-Sector Challenges, and Policy Recommendations

The actual implementation of cloud security strategies across various sectors shows variability in outcomes based on the level of organizational readiness, infrastructure, and compliance with security controls. In the healthcare sector, the use of the cloud enables quick access to patient medical records and effective telemedicine services. However, vulnerability to health data theft remains high. Noted that 23% of attacks on global healthcare systems in 2021 originated from cloud exploitation, emphasizing the need for strong encryption and data segmentation. The financial sector shows more aggressive attack dynamics, with a 54% increase in cloud-targeted attacks on financial institutions. Banks and fintech companies require AI-based fraud detection systems and data tokenization to secure digital transactions. This experience confirms that each sector requires a cloud security model tailored to its specific risk characteristics.

Table 2. Cross-Sector Cloud Security Implementation Maturity Comparison

Sector	Key Cloud Uses	Common Threats	Security Maturity Level	Primary Security Controls
Healthcare	Electronic health records, telemedicine	Data breaches, ransomware	Medium	Encryption, access segmentation, audit logging
Financial services	Digital banking, payment processing	Fraud attacks, phising, cloud malware	High	AI-based fraud detection, tokenization, MFA, ZTA
Education	Cloud learning	Credential theft,	Low-	IAM, password

	platforms, student data systems	ransomware	Medium	policy enforcement, user awareness training
Public Sector	E-government services, identity registries	Mass DDoS, data exfiltration	Low-Medium	Government security standards, SOC monitoring
SMEs	SaaS business tools, cloud storage	Misconfiguration, credential compromise	Low	Basic encryption, shared cloud security tools

Note: Security maturity levels categorized based on control depth, automation, incident response capability, and compliance alignment.

In the education sector, the pandemic has accelerated the adoption of cloud learning platforms, but ransomware and credential-based attacks remain major challenges (Adelusi et al., 2022). Educational institutions that are less mature in terms of governance and digital literacy are often targeted by attacks that exploit the credential weaknesses of students and staff. In the government sector, the digitization of public services, including digital identity systems and administrative databases, requires cloud systems that are secure and comply with national security standards. A report by BSSN (2023) noted that more than 361 million cyber attacks targeted the Indonesian public sector, highlighting the urgent need to improve the government's digital security capabilities. The successful implementation of cloud computing in the public sector is greatly influenced by the integration of security-by-design in every stage of digital service system development.

Significant challenges in implementing cloud security in developing countries include budget constraints, lack of IT infrastructure, and a shortage of digital security personnel. Silitonga, (2023) highlight that organizations in Indonesia face structural challenges in the form of a technical skills gap and a lack of security culture. To overcome this, a strategic approach to digital workforce training and long-term investment in threat detection systems are needed. National cybersecurity training programs are an important step in strengthening the country's digital resilience. IBM Security (2023) asserts that organizations that build comprehensive training programs experience a 45% reduction in incidents due to human error.

In addition, the maturity of incident management procedures also determines the effectiveness of responses to cloud threats. Research by Xiao and Watson (2019) shows that organizations with a formal incident response framework are able to shorten attack mitigation time by up to 60%. Organizational resilience must involve rapid data recovery mechanisms, system audits, and regular threat simulations to test operational responses. At the public policy level, the government needs to strengthen collaboration with the private sector and the

digital security professional community to promote standardization and threat intelligence sharing. Such collaborative strategies are important to address the information gap regarding cyber attacks.

Going forward, cloud security strategies must be developed into an adaptive cloud security framework that combines AI-driven automation, ZTA, encryption-as-a-service, and multi-layer governance. The integration of cloud-native technologies such as container security, DevSecOps, and continuous compliance monitoring will also be the foundation for building a zero trust continuous validation-based computing security architecture. This holistic approach allows organizations to continuously adapt their security strategies to technological developments and threats.

Thus, cloud security implementation requires comprehensive synergy between technology, governance, human resources, and public policy to protect information integrity. Secure cloud adoption not only results in operational efficiency and digital progress but also increases public trust in the national digital ecosystem. This success will strengthen Indonesia's digital competitiveness in the era of data-based economic globalization (Sahetapy et al., 2025).

CONCLUSION

This study confirms that information security in the cloud environment is a strategic aspect that is inseparable from digital transformation in the modern era. A literature review shows that cloud computing brings significant benefits in terms of scalability, efficiency, and innovation in cross-sector digital services, but also presents increasingly complex security risks. The main challenges identified in cloud security implementation include rapidly evolving cyber threats, system configuration errors, weaknesses in identity access management, and gaps in human resource skills in digital security. Various technological strategies such as Zero Trust Architecture, advanced encryption, and artificial intelligence-based threat monitoring have proven effective in mitigating risks. However, the effectiveness of security controls is not only determined by technology, but also by the synergy of governance policies, regulatory compliance, and organizational readiness to integrate security practices comprehensively into digital operations.

Thus, cloud security is a dynamic process that requires a holistic and adaptive approach. In line with these findings, this study confirms that the successful implementation of cloud security strategies is increasingly determined by human factors and institutional governance. Cybersecurity literacy training programs, increased digital awareness, and strengthened governance are essential elements in creating a reliable and secure cloud environment.

It is also important for organizations to implement a risk-based security governance framework, improve real-time threat monitoring capabilities, and align internal policies with national regulations and international standards. The challenges faced by developing countries such as Indonesia, including

limited technical resources and digital infrastructure, demonstrate the need for strong public policy direction to promote the harmonization of effective and sustainable cloud security standards. In addition, collaboration between the public, private, and academic sectors is a key instrument in accelerating the improvement of national digital security resilience.

34 Based on the results of the study, the recommendations include the development of an adaptive cloud security framework that integrates Zero Trust, DevSecOps, and AI technology for continuous threat detection. Organizations need to build internal security capacity through ongoing training programs, periodic risk assessments, and incident response simulations. The government also needs to strengthen national digital security policies, ensure public and private sector compliance with cloud security standards, and facilitate the acceleration of compliance automation adoption. By implementing an integrated approach between technology, regulation, and human resource capacity building, organizations and countries can improve digital resilience and build public trust in the safe and responsible use of cloud services.

REFERENCES

Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and Ubiquitous Computing*, *28*(1), 59–72. https://doi.org/10.1007/s00779-021-01583-8

Abdulsalam, Y. S., & Hedabou, M. (2021). Security and Privacy in Cloud Computing: Technical Review. *Future Internet*, *14*(1), 11. https://doi.org/10.3390/fi14010011

Adejumo, A. P., & Ogburie, C. P. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(3), 1542–1556. https://doi.org/10.30574/wjarr.2025.25.3.0909

Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2022). Advances in Cybersecurity Strategy and Cloud Infrastructure Protection for SMEs in Emerging Markets. *Journal of Frontiers in Multidisciplinary Research*, *3*(1), 467–482. https://doi.org/10.54660/.JFMR.2022.3.1.467-482

Adeusi, O. C., Adebayo, Y. O., Ayodele, P. A., Onikoyi, T. T., Adebayo, K. B., & Adenekan, I. O. (2024). IT standardization in cloud computing: Security challenges, benefits, and future directions. *World Journal of Advanced Research and Reviews*, *22*(3), 2050–2057. https://doi.org/10.30574/wjarr.2024.22.3.1982

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics*, *11*(1), 16. https://doi.org/10.3390/electronics11010016

Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *Journal of Information Security*, *15*(02), 148–167. https://doi.org/10.4236/jis.2024.152010

Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Al-rimy, B. A. S. (2021). Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and

Open Challenges. *Applied Sciences*, *11*(19), 9005. https://doi.org/10.3390/app11199005

Ang'udi, J. J. (2023). Security challenges in cloud computing: A comprehensive analysis. *World Journal of Advanced Engineering Technology and Sciences*, *10*(2), 155–181. https://doi.org/10.30574/wjaets.2023.10.2.0304

Arumugam, K. J. (2025). *Behind the Cloud: Uncovering Critical Security Threats*. SSRN. https://doi.org/10.2139/ssrn.5160686

Baladari, V. (2024). *ENHANCING PERFORMANCE AND SECURITY IN MULTI-CLOUD AND HYBRID-CLOUD ENVIRONMENTS*. https://doi.org/10.5281/ZENODO.15020436

Bishukarma, R. (2023). Scalable Zero-Trust Architectures for Enhancing Security in Multi-Cloud SaaS Platforms. *International Journal of Advanced Research in Science, Communication and Technology*, 1308–1319. https://doi.org/10.48175/IJARSCT-14000S

Budiardjo, A., Nugroho, & Reksodiputro. (2019, October 30). *Indonesia Issues Important New Regulation on Electronic (Network and Information) Systems*. ABNR - Counsellors at Law. https://www.abnrlaw.com/news/indonesia-issues-important-new-regulation-on-electronic-network-and-information-systems

Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*, *3*(3), 422–450. https://doi.org/10.3390/network3030018

Check Point Software Technologies Ltd. (2025, November 24). *Cloud-based Cyberattacks Increased by 48% in 2022, as Hackers Continue to Leverage Digital Transformation*. Global Security Mag Online. https://www.globalsecuritymag.com/Cloud-based-Cyberattacks-Increased-by-48-in-2022-as-Hackers-Continue-to.html

El-Bably, A. Y. (2021). Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management. *Journal of Information Security and Cybercrimes Research*, *4*(1), 95–102. https://doi.org/10.26735/WLPW6121

Eleweke, I., Umakor, M. F., Ndubuisi, C. W., Amomo, C. G., Adeniji, S., & Temidayo, M. (2025). Ai-Driven Threat Detection and Prevention in Cloud Computing Environments. *American Journal of Innovation in Science and Engineering*, *4*(3), 49–56. https://doi.org/10.54536/ajise.v4i3.5041

Faisal, N. A., Nahar, J., Graduate Research Assistant, Department of Finance, Louisiana State University, Baton Rouge, Louisiana, USA, Sultana, N., Master in Management Information Systems, College of Business, Lamar University, Beaumont, USA, Mintoo, A. A., & Graduate student, School of Computer and Information Sciences, Washington University of Science and Technology (WUST), USA. (2024). Fraud Detection In Banking Leveraging Ai To Identify And Prevent Fraudulent Activities In Real-Time. *Non Human Journal*, *1*(01), 181–197. https://doi.org/10.70008/jmldeds.v1i01.53

Gupta, N., Agrawal, R., & Arora, K. (2025). Cloud Computing in Healthcare: Risks and Security Measures. In R. Agrawal, P. S. Rathore, G. G. Devarajan, & R. R. Divivedi (Eds.), *Artificial Intelligence and Cybersecurity in Healthcare* (1st ed., pp. 221–242). Wiley. https://doi.org/10.1002/9781394229826.ch9

Hamza, R., Hassan, A., Ali, A., Bashir, M. B., Alqhtani, S. M., Tawfeeg, T. M., & Yousif, A. (2022). Towards Secure Big Data Analysis via Fully Homomorphic Encryption Algorithms. *Entropy*, *24*(4), 519. https://doi.org/10.3390/e24040519

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Husriadi, Muh., Bahar, H., & Windayani, W. (2024). CRITICAL REVIEW OF THE USE OF BLOCKCHAIN TECHNOLOGY IN IMPROVING MSME DATA TRANSPARENCY AND SECURITY. *Journal of Finance, Economics and Business*, *3*(1), 53–60. https://doi.org/10.59827/jfeb.v3i1.107

Kadbe, P. K., Patil, B. H., Piske, R. S., & Patil, R. B. (2025). Malicious usage of artificial intelligence: Expansion of existing threats and novel threats. In *Artificial Intelligence for Cyber Security and Industry 4.0*. CRC Press.

Karagiannis, C., & Vergidis, K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information*, *12*(5), 181. https://doi.org/10.3390/info12050181

Katuk, N., Zaimy, N. A. ' F., Krishnan, S., Kunhiraman, R. K., Lee, H.-H., & Eleyan, D. (2024). Fostering Cyber-Resilience in Higher Education: A Pilot Evaluation of a Malware Awareness Program for College Students. In N. H. Zakaria, N. S. Mansor, H. Husni, & F. Mohammed (Eds.), *Computing and Informatics* (Vol. 2002, pp. 154–167). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-9592-9_12

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Khan, S. U., Khan, H. U., Ullah, N., & Khan, R. A. (2021). Challenges and Their Practices in Adoption of Hybrid Cloud Computing: An Analytical Hierarchy Approach. *Security and Communication Networks*, *2021*, 1–20. https://doi.org/10.1155/2021/1024139

Kumar, K. J., Sai, K. A., Reddy, A. D., Daiwik Reddy, C. P., & Rajagopal, S. M. (2025). A Comprehensive End-to-End Solution for Web Security with Cryptography, Multi-Factor Authentication, and Secure Communication. *2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, 325–332. https://doi.org/10.1109/IDCIOT64235.2025.10915145

MarketsandMarkets Research Pvt. Ltd. (2023, August 16). *Public Cloud Market worth $987.7 billion by 2027, growing at a CAGR of 17.3 % Report by MarketsandMarkets™*. https://finance.yahoo.com/news/public-cloud-market-worth-987-140000910.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAADvhqxESU5ZytB14_YEcQdKXSW5dxIgxqZH9iXMoMsJUxKxKbGavMuFPeDVBG5v4EqzqkFkTfJwuCjcon30kaMkVmGYLyS_zGgAVXqsULQnKDoWaUsIpOw99arCOXM_F1UVhA5QXdb9FaErm-bspbvx9D2Sjz8PiLaa4khU6FmCn

Mortimer, J. (n.d.). *Cybersecurity for Sustainable and Digital Economic Transformations*.

Odetunde, A., Adekunle, B. I., & Ogeawuchi, J. C. (2022). Using Predictive Analytics and Automation Tools for Real-Time Regulatory Reporting and Compliance Monitoring. *International Journal of Multidisciplinary Research and Growth Evaluation*, *3*(2), 650–661. https://doi.org/10.54660/.IJMRGE.2022.3.2.650-661

Oladosu, S. A., Ike, C. C., Adepoju, P. A., Afolabi, A. I., Ige, A. B., & Amoo, O. O. (2021). Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premise integrations. *Magna Scientia Advanced Research and Reviews*, *3*(1), 079–090. https://doi.org/10.30574/msarr.2021.3.1.0076

Pandya, U. (2025, May 18). Enhancing Cloud Security and Compliance through Artificial Intelligence: A Conceptual Framework. *International Conference on Computer Science, Artificial Intelligence, Machine Learning [ICCSAIML'25]*. International Conference on Computer Science, Artificial Intelligence, Machine Learning. https://doi.org/10.56472/ICCSAIML25-135

Rasner, G. C. (2021). *Cybersecurity and Third-Party Risk: Third Party Threat Hunting*. https://books.google.co.id/books?hl=en&lr=&id=mw8zEAAAQBAJ&oi=fnd&pg=PT6&dq=digital+supply+chain+attacks+have+increased+by+300%25+in+the+last+five+years,+with+many+cases+related+to+intrusions+into+third-party+systems+that+then+affect+end+users&ots=av5B5NEztB&sig=iJQVcWQPMqQ4YPHXcb_0KZa0IZE&redir_esc=y#v=onepage&q&f=false

Rawal, B. S., Manogaran, G., & Peter, A. (2023). *Cybersecurity and Identity Access Management*. Springer Nature Singapore. https://doi.org/10.1007/978-981-19-2658-7

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries. *Computers*, *10*(11), 150. https://doi.org/10.3390/computers10110150

Richard Arogundade, O. (2023). Strategic Security Risk Management in Cloud Computing: A Comprehensive Examination and Application of the Risk Management Framework. *IARJSET*, *11*(1). https://doi.org/10.17148/IARJSET.2024.11105

Rusydi, M. T. (2025). Cyber Law Policy Development: Indonesia's Response to International Cybercrime Threats. *Journal of Progressive Law and Legal Studies*, *3*(01), 69–85. https://doi.org/10.59653/jplls.v3i01.1365

Sahetapy, H., Halik, M. Y., Sino, H. W., & Bokau, J. R. S. (2025). Big Data and Artificial Intelligence: Implications and Strategies for Business Development in Indonesia. *Journal of Marketing Management and Innovative Business Review*, *3*(1), 65–77. https://doi.org/10.63416/mrb.v3i1.321

Sam, D., Nithya, K., Kanmani, S. D., Sheeba, A., Ebenezer, A. S., Maheswari, B. U., & Amesh, J. D. (2023). Survey of risks and threats in online learning applications. In L. J. Deborah, P. Vijayakumar, B. B. Gupta, & D. Pelusi, *Secure Data Management for Online Learning Applications* (1st ed., pp. 31–47). CRC Press. https://doi.org/10.1201/9781003264538-2

Santos, A., Martins, J., Duarte Pestana, P., Gonçalves, R., São Mamede, H., & Branco, F. (2024). Factors Affecting Cloud Computing Adoption in the Education Context—Systematic Literature Review. *IEEE Access*, *12*, 71641–71674. https://doi.org/10.1109/ACCESS.2024.3400862

Silitonga, M. S. (2023). The Public Sector's Digital Skills Gap in Indonesia: The Challenges and Opportunities. *Jurnal Good Governance*, 70–79. https://doi.org/10.32834/gg.v19i1.585

Singh, U. K., & Sharma, A. (2021). Cloud Computing Security Framework Based on Shared Responsibility Models. In V. Bali, V. Bhatnagar, D. Aggarwal, S. Bali, & M. J. Diván, *Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0* (1st ed., pp. 39–55). CRC Press. https://doi.org/10.1201/9781003146711-3

Smita Verma. (2025). Cybersecurity compliance in the age of remote work: Challenges and solutions. *World Journal of Advanced Engineering Technology and Sciences*, *15*(1), 1112–1120. https://doi.org/10.30574/wjaets.2025.15.1.0286

Stewart, H. (2023). Digital Transformation Security Challenges. *Journal of Computer Information Systems*, *63*(4), 919–936. https://doi.org/10.1080/08874417.2022.2115953

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, *10*, 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

Vashishth, T. K., Sharma, V., Sharma, K. K., Kumar, B., Chaudhary, S., & Panwar, R. (2025). Securing the Cloud: Strategies for Protecting Sensitive Patient Data in Cloud-Based Healthcare Recommender Systems. In S. P. Singh, D. K. Jain, & J. Debayle (Eds.), *Healthcare Recommender Systems* (pp. 185–220). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-80056-6_9

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, *16*(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995