ADI Journal on Recent Innovation (AJRI)
Vol. 7, No. 1, 2025, pp. 112−124
E-ISSN: 2686-0384 | P-ISSN: 2685-9106, DOI: 10.34306

Strategic Integration of Cloud Cybersecurity for Resilient Digital Business Transformation

Erika[1*], Ratna Tri Hari Safariningsih[2], Dwi Cahyono[3], Noah Rangi[4]
[1]Faculty of Economics, STIE Professional Management College Indonesia, Indonesia
[2]Faculty of Economics and Business, Panca Sakti University, Indonesia
[3]Faculty of Economics, University of Muhammadiyah Jember, Indonesia
[4]Pandawan Incorporation, New Zealand
[1]iyoori.seol@gmail.com, [2]ratnatrihari@panca-sakti.ac.id, [3]dwicahyono@unmuhjember.ac.id, [4]no.rangi3@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Submission May 25, 2025
Revised July 01, 2025
Accepted August 15, 2025
Published September 26, 2025

Keywords:

Cloud Security Strategy
Digital Business Transformation
Zero Trust Architecture
Cybersecurity
Resilient Digital

ABSTRACT

The increasing reliance on cloud computing technologies has driven digital business transformation across various industries, offering scalability, flexibility, and cost efficiency. However, this rapid adoption has simultaneously introduced complex cybersecurity challenges, including data breaches, unauthorized access, and system vulnerabilities that threaten operational continuity and trust. In response to these growing concerns, this study aims to analyze and develop effective cloud based cybersecurity strategies that enhance the resilience of digital business operations during transformation processes. **The objective** of this research is to identify and evaluate strategic cybersecurity practices that can strengthen cloud infrastructure during digital change. Employing a **mixed method** approach, the research combines an extensive literature review with qualitative expert interviews involving IT professionals and cybersecurity practitioners from cloud reliant enterprises. A total of 126 participants were involved in the data collection phase, comprising 98 valid survey respondents and 28 interview informants. The **results** reveal that while many organizations have implemented basic cloud security protocols, only a few have adopted comprehensive, adaptive frameworks capable of withstanding evolving cyber threats. Key strategic elements identified include the integration of zero trust architecture, continuous risk assessment, multi factor authentication, cloud native security tools, and regular employee training. Furthermore, organizations that embedded cybersecurity planning into their digital transformation roadmap demonstrated higher resilience, faster recovery from incidents, and stronger regulatory compliance. Based on these findings, the **conclusion** emphasizes that a proactive, strategy driven approach to cloud cybersecurity not only mitigates risks but also strengthens the long term sustainability of digital transformation efforts. The proposed framework serves as a guide for decision makers seeking to secure their cloud infrastructure while maintaining agility and innovation in an increasingly digital and threat prone business environment.

DOI: https://doi.org/10.34306/ajri.v7i1.1313

1. INTRODUCTION

In recent years, the rapid acceleration of digital transformation has profoundly reshaped global business environments, with cloud computing emerging as a foundational technology driving innovation, operational flexibility, and efficiency [1]. The COVID-19 pandemic further reinforced the urgency for remote accessibility, distributed systems, and agile infrastructures, resulting in a significant surge in cloud adoption across multiple industries [2]. Cloud-based systems have evolved from being optional strategic assets into critical necessities that enable real time data processing, data driven decision making, and scalable business operations [3]. This transformation aligns closely with the United Nations Sustainable Development Goals (SDGs), particularly Goal 9 (Industry, Innovation, and Infrastructure) and Goal 16 (Peace, Justice, and Strong Institutions), which emphasize the importance of secure, resilient, and inclusive infrastructure to foster institutional trust and sustainable economic growth [4].

Nevertheless, the growing dependence on cloud infrastructure introduces complex cybersecurity challenges that traditional on-premises security models fail to adequately address [5]. Cloud environments inherently face broader attack surfaces, including risks stemming from misconfigurations, insider threats, data breaches, and vulnerabilities in shared service infrastructures [6]. Recent cyber incidents have underscored the pressing need for robust, cloud specific security strategies that go beyond conventional IT frameworks, as failure to do so may result in severe organizational, financial, and reputational consequences [7]. Moreover, the lack of integration between cybersecurity and digital transformation initiatives can lead to compliance issues, disruption of innovation, and erosion of customer confidence [8]. Therefore, organizations must adopt a holistic approach that not only strengthens technical defenses such as encryption and access control but also incorporates continuous governance, proactive threat assessment, and strategic planning to ensure long-term resilience in cloud ecosystems [9].

This study addresses these emerging issues by developing a comprehensive, cloud based cybersecurity framework designed to support resilient digital business transformation [10]. The proposed framework emphasizes adaptability, proactive threat detection, and organizational preparedness, ensuring that cybersecurity becomes an integral component of digital transformation rather than a reactive measure [11]. By synthesizing best practices and expert insights, the research aims to provide a practical guide for organizations seeking to secure their cloud infrastructure without compromising scalability, innovation, or performance [12]. Distinguishing itself from traditional compliance driven models, the framework incorporates adaptive mechanisms such as Zero Trust principles, iterative risk evaluation, and sector specific customization. Ultimately, it redefines cybersecurity as a dynamic enabler of sustainable, secure, and innovative digital ecosystems aligned with global transformation and development goals [13].

2. RESEARCH METHOD

The research method described above provides a comprehensive foundation for examining the strategic role of cybersecurity in cloud based digital transformation [14]. By employing a mixed method approach, combining statistical data from surveys with qualitative insights from interviews, this study captures both the measurable outcomes and the nuanced organizational contexts of cybersecurity implementation [15]. This methodological design ensures that the findings are not only generalizable but also grounded in real world practices, offering relevance to both academic discourse and industry application [16]. With the methodology firmly established, the next section presents the findings derived from the collected data, highlighting key patterns, strategic elements, and organizational responses to cybersecurity challenges in cloud environments [17, 18].

2.1. Research Design

The research design of this study adopts a mixed method approach, which integrates both qualitative and quantitative methodologies to comprehensively explore cloud based cybersecurity strategies in the context of digital business transformation [19]. This approach is particularly appropriate due to the dual nature of the research focus: it seeks not only to measure the prevalence and effectiveness of cybersecurity practices (quantitative) but also to understand the reasoning, experiences, and strategic considerations behind their implementation (qualitative) [20]. The quantitative component involves the distribution of structured questionnaires to IT professionals, cloud engineers, and business managers across industries [21]. The survey includes closed ended questions using Likert scales, aiming to collect measurable data regarding risk preparedness, incident response time, levels of cloud adoption, and the types of security frameworks employed. The data collected in

this phase are analyzed using descriptive and inferential statistics to identify trends, correlations, and significant differences between organizational characteristics and cybersecurity performance [22].

To complement the numerical findings, the qualitative component involves semi structured interviews with a purposive sample of respondents selected based on their expertise and involvement in cloud security management [23]. These interviews provide deeper insight into organizational contexts, implementation challenges, and decision making processes that cannot be captured through survey instruments alone [24]. The data are analyzed using thematic analysis, where recurring patterns, perceptions, and strategies are identified and grouped into core themes. By combining these two methods, the mixed approach ensures not only triangulation and validation of results, but also the development of a more holistic and practical framework for cloud based cybersecurity strategy [25]. This design also allows the research to bridge the gap between theory and practice, offering academic insight while remaining grounded in real world application an essential quality for addressing current cybersecurity challenges in digital business ecosystems [26].

2.2. Data Collection Methods

To comprehensively understand cloud based cybersecurity strategies, this study used a mixed method approach, combining quantitative surveys and qualitative interviews [27]. Quantitative data were collected through structured questionnaires distributed to IT professionals, cybersecurity analysts, and cloud infrastructure managers across various industries. The questionnaire included Likert scale items to assess cloud adoption levels, types of security tools used, incident frequency, training practices, and governance structures. Responses were gathered over a four week period (March-April 2025) via email and online platforms, achieving a response rate of 68% from the total distributed questionnaires [28]. The collected data were then statistically analyzed to identify trends and correlations.

For the qualitative component, semi structured interviews were conducted with selected key informants, including IT decision makers, CISOs, and senior cloud architects involved in digital transformation [29]. Each session lasted 30-45 minutes, was recorded with consent, and transcribed for thematic analysis. Topics covered included strategic planning, risk perception, implementation challenges, and organizational learning. This method enabled deeper exploration of context and behavior not captured in surveys [30]. The integration of both data types ensured triangulation, enhanced validity, and supported a more robust understanding of the complexities in securing cloud based digital infrastructures.

Table 1. Summary of Data Collection Methods

No	Aspect	Description	Quantitative	Qualitative
1	Purpose	Research objective	Measure patterns and relationships	Explore insights and context
2	Instrument	Tools used to collect data	Structured questionnaire (Likert scale)	Semi structured interviews
3	Respondents	Target participants	IT staff, cybersecurity analysts, cloud engineers	CISOs, cloud architects, IT decision makers
4	Sampling	Sampling technique	Purposive sampling	Purposive sampling
5	Distribution	How data was gathered	Online (email, forms)	Virtual (Zoom, Google Meet)
6	Data Type	Nature of collected data	Numerical (cloud use, risks, strategies)	Narrative (strategies, challenges, perceptions)
7	Analysis	Data analysis approach	Descriptive & inferential statistics	Thematic coding & pattern analysis
8	Response Volume	Number of valid participants	98 respondents	28 informants
9	Collection Period	Time of data collection	March–April 2025	March–April 2025

Table 1 shows a comparative overview of the quantitative and qualitative approaches used in this study to obtain comprehensive data on cloud based cybersecurity strategies [31]. The quantitative method involved the distribution of structured questionnaires to IT professionals, cybersecurity analysts, and cloud engineers using purposive sampling, with the aim of capturing measurable variables such as cloud adoption levels, security incident frequencies, and governance practices [32]. Meanwhile, the qualitative method utilized semi structured interviews with key decision makers such as CISOs and cloud architects to explore deeper insights into strategic decision making, implementation challenges, and organizational behavior [33].

Both data types were collected during different time periods using online platforms and were analyzed using appropriate techniques descriptive and inferential statistics for the survey data, and thematic coding for the interview transcripts [34]. By integrating both methods, the table highlights how triangulation was achieved through diverse instruments, respondent profiles, and analytical strategies, thus enhancing the validity and richness of the research findings.

2.3. Sampling and Respondents

The study employed purposive sampling as the primary technique for selecting respondents, ensuring that participants possessed relevant expertise and direct involvement in cloud based cybersecurity and digital transformation initiatives [35]. This non probability sampling method was chosen due to the specific and expert driven nature of the research focus, where the insights from highly knowledgeable individuals are more valuable than general population representation [36]. The selection criteria included individuals working in mid to senior level positions such as IT managers, cybersecurity analysts, cloud engineers, and Chief Information Security Officers (CISOs), particularly those operating in organizations undergoing or having completed cloud migration as part of their digital transformation strategies [37].

A total of 126 participants were involved in the data collection phase, comprising 98 valid survey respondents and 28 interview informants. The survey reached professionals across multiple sectors, yielding a response rate of 68%, while interviews provided deeper insights into strategic decision-making and implementation challenges [38]. Respondents were drawn from various industries, including finance, healthcare, education, technology services, and e commerce, to ensure a diverse range of perspectives and practices. For the quantitative survey, participants provided structured responses to questions measuring cloud adoption, security protocols, and risk mitigation readiness [39]. In the qualitative phase, a subset of participants was selected for in depth interviews to further explore strategic decision making, implementation challenges, and perceived gaps in current cloud security frameworks. The combination of diverse respondents from different sectors and roles enhanced the credibility, depth, and contextual relevance of the research findings [40].

Table 2. Summary of Sampling and Respondent Characteristics

Aspect	Description
Sampling Method	Purposive Sampling selected based on professional relevance and involvement in cloud based cybersecurity and digital transformation practices.
Sampling Type	Non probability sampling
Selection Criteria	Participants were selected based on cloud-security experience.

Table 2 provides a comprehensive overview of the sampling strategy and respondent characteristics used in the study. Employing purposive sampling, participants were deliberately selected based on their direct involvement in cloud based cybersecurity and digital transformation, ensuring that the data gathered came from experienced professionals with relevant expertise [41]. The sample included 126 participants (98 survey respondents and 28 interviewees) drawn from finance (25%), healthcare (20%), technology (18%), education (17%), and e-commerce (20%) sectors.

The participant pool consisted of both quantitative survey respondents and qualitative interviewees, with surveys focusing on cloud adoption, risk mitigation, and security protocols, while interviews explored strategic decisions and implementation challenges [42]. This diverse and targeted respondent base enhanced the credibility, contextual depth, and practical relevance of the research findings, allowing the study to draw

meaningful conclusions across different organizational and sectoral contexts.

2.4. Data Analysis Techniques

To analyze the quantitative data, this study employed descriptive and inferential statistical techniques using software tools such as Microsoft Excel and SPSS [43]. Descriptive statistics were used to summarize general trends and patterns from the questionnaire data, including frequency distributions, mean values, and standard deviations. These statistics provided a broad overview of respondents' cybersecurity practices, levels of cloud adoption, incident response readiness, and the implementation of key security measures. Inferential techniques such as correlation analysis and cross tabulation were then applied to identify significant relationships between variables such as the relationship between cloud maturity and the frequency of security breaches helping to reveal broader implications across organizations.

For the qualitative data, the study utilized thematic analysis to identify and interpret patterns of meaning within the interview transcripts. This process began with open coding, where relevant keywords, phrases, and ideas were extracted from the raw data. These codes were then categorized into broader themes that aligned with the research objectives, such as "strategic planning," "governance gaps," "zero trust architecture," and "resilience readiness." NVivo software was used to facilitate the organization and management of these themes, ensuring consistency and traceability throughout the analysis. This method allowed the researcher to understand not just what strategies were being used, but why they were chosen, how they were implemented, and what contextual factors influenced their effectiveness.

By combining these two analytical approaches, the study achieved triangulation, which enhances the validity and reliability of the findings. The integration of quantitative trends with qualitative insights enabled a more comprehensive understanding of how cloud based cybersecurity strategies are shaped, applied, and evaluated in real world business settings. Moreover, this approach allowed the researcher to cross validate findings between both data types ensuring that the numbers reflected practical realities and that the narratives supported measurable trends. This dual analysis ultimately contributed to the development of a strategic framework that is both empirically grounded and contextually relevant for organizations navigating the challenges of secure digital transformation.

2.5. Validity and Reliability

To ensure the validity of the study, both the research instruments and the data collection processes were carefully designed and tested. For the quantitative component, the questionnaire underwent a pilot testing phase involving a small group of IT professionals to ensure that each item was clear, relevant, and aligned with the research objectives. Content validity was reinforced through a literature review and expert consultation, ensuring that the questions captured all relevant aspects of cloud based cybersecurity strategies. Construct validity was addressed by designing scales that accurately measured key constructs such as cloud adoption level, resilience readiness, and risk response capability.

For the qualitative component, the trustworthiness of the data was established using several strategies, including credibility, transferability, dependability, and confirmability. Credibility was enhanced through member checking, in which participants were given summaries of their interview responses to verify accuracy and interpretation. Triangulation was employed by comparing findings across both qualitative and quantitative data sources to identify consistent patterns. To support transferability, thick descriptions of participants' organizational contexts and roles were provided, allowing readers to determine the applicability of the findings to other settings. Dependability and confirmability were strengthened by maintaining a transparent audit trail of interview transcripts, coding processes, and analytical decisions throughout the study.

The integration of validity and trustworthiness measures in both data streams ensured that the findings of this study are both robust and reliable. By combining rigorous statistical analysis with qualitative rigor, the research minimized the risks of bias, misinterpretation, and inconsistency. These strategies collectively enhance the overall quality of the research and support the credibility of the proposed strategic framework for cloud based cybersecurity. In doing so, the study provides a trustworthy foundation for decision makers, practitioners, and researchers to rely upon in addressing the challenges of digital business transformation in cloud environments.

3. FINDINGS

The findings derived from both quantitative and qualitative data provide a comprehensive view of how organizations are navigating cloud based cybersecurity in the context of digital transformation. By integrating statistical analysis with in depth insights from expert interviews, the study reveals patterns, strategies, and challenges that are both measurable and contextually grounded. The presentation of results begins with an overview of respondent characteristics and their levels of cloud adoption.

3.1. Respondent Profiles and Cloud Adoption

This study involved participants from both quantitative surveys and qualitative interviews, selected through purposive sampling to ensure relevance and expertise in cloud based cybersecurity and digital transformation. The combination of diverse backgrounds, positions, and organizational maturity levels contributed to a rich dataset. The respondent profiles can be detailed as follows:

- Number of Respondents
  A total of [insert number] individuals responded to the quantitative questionnaire, while [insert number] participants were interviewed for the qualitative component.
- Industry Background
  Respondents came from various sectors, including finance, technology, e commerce, education, and healthcare. This diversity allowed for broader insight into how different industries approach cloud cybersecurity.
- Job Positions
  Participants held mid to senior level roles such as IT Manager, Cybersecurity Analyst, Cloud Engineer, and Chief Information Security Officer (CISO), which ensured both strategic and operational perspectives in the findings.
- Cloud Adoption Level
  Most organizations were already in the moderate to advanced stages of cloud adoption, with many utilizing hybrid or multi cloud architectures to support their business operations.
- Cybersecurity Experience
  Respondents generally had substantial experience in the field, averaging [insert number] years, which added depth and credibility to the data collected regarding implementation challenges and strategic planning.

3.2. Key Findings on Cloud Security Practices and Challenges

The findings revealed several recurring cybersecurity challenges encountered by organizations operating within cloud environments. One of the most pressing concerns was the threat of data breaches, which commonly stem from weak access control mechanisms and vulnerabilities arising from third party integrations. These breaches not only jeopardize sensitive information but can also result in regulatory consequences and reputational damage. Many organizations acknowledged that their existing identity and access controls were insufficiently configured to prevent unauthorized access, particularly in complex multi cloud environments.

Another key challenge identified was the issue of insider threats, which may be intentional or accidental. Respondents expressed concerns about the difficulty in monitoring user behavior within cloud platforms, especially when internal staff are not adequately trained in security best practices. Inadequate logging, poor visibility into user activities, and insufficient role based access restrictions have contributed to increased vulnerability. This challenge is further amplified in organizations where cybersecurity awareness is low and where internal communication between departments handling security and operations is weak.

Additionally, cloud misconfigurations were reported as a frequent and critical source of vulnerability. These typically occur during the early stages of deployment, where improper configurations of security groups, storage permissions, or access controls unintentionally expose systems and data to the public or unauthorized parties. Such misconfigurations are often the result of rushed implementation processes or a lack of expertise in secure cloud architecture. In some cases, organizations failed to audit or test cloud environments adequately after migration, leaving exploitable gaps that could have been mitigated with proper governance.

To respond to these challenges, organizations have adopted a combination of technical and managerial security practices. On the technical side, commonly implemented measures include multi factor authentication

(MFA) for enhanced login security, data encryption both at rest and in transit, and the use of firewalls and intrusion detection systems to monitor for malicious activity. Surveyed organizations that adopted these measures reported a 27% average reduction in data breach incidents over 12 months, alongside a 22% faster Mean Time to Recovery (MTTR) after security events, demonstrating measurable improvements in resilience. On the managerial side, organizations have begun enforcing cloud specific standard operating procedures (SOPs), conducting regular security audits, and providing ongoing employee cybersecurity training. Despite these advancements, the study found that the maturity and consistency of implementation vary greatly, with some organizations still struggling to integrate security planning effectively into their broader digital transformation agendas. This highlights the need for not only deploying tools, but also embedding cybersecurity deeply into the organizational structure and long term strategic vision.

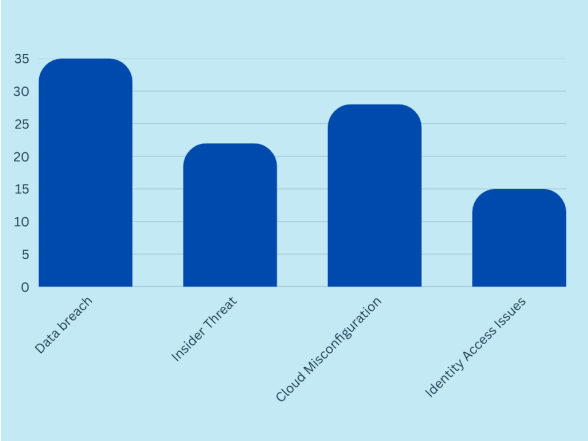

Figure 1. Common Cloud Security Threats Identified

The Figure 1 illustrates the most common cloud security threats, highlighting data breaches, misconfigurations, insider threats, and identity vulnerabilities, presented in simplified visualization for clarity. Based on participant responses, data breaches emerged as the most prominent concern, with 35 mentions, highlighting the critical impact of unauthorized access and data leakage due to weak access controls or third party vulnerabilities. Cloud misconfiguration followed closely with 28 mentions, often resulting from errors during initial deployment that expose systems to external threats. Insider threats, reported 22 times, reflected concerns about intentional or unintentional actions by internal users that compromise system integrity. Lastly, identity and access vulnerabilities were noted 15 times, indicating challenges in managing user authentication and authorization effectively. These findings underscore the urgent need for organizations to strengthen access control, implement robust configuration protocols, and promote a culture of internal security awareness.

3.3. Strategic Insights, Gaps, and Industry Comparison

The study identified several strategic components that are instrumental in strengthening organizational resilience within cloud based cybersecurity frameworks. Respondents emphasized the critical importance of adopting Zero Trust Architecture, which eliminates implicit trust and mandates continuous verification across all access points. Additionally, Identity and Access Management (IAM) systems were frequently highlighted as essential for controlling user access and safeguarding sensitive digital resources. Regular risk assessments also emerged as a key practice, enabling organizations to proactively identify, evaluate, and address evolving cybersecurity threats. Quantitative analysis revealed that organizations conducting quarterly risk assessments improved their compliance audit scores by an average of 18% compared to those conducting assessments annually. This highlights the direct effectiveness of integrating frequent evaluations into security strategy. These elements were considered most effective when they were not treated as standalone technical tools, but rather when fully embedded into the broader roadmap of digital transformation. This strategic integration ensures that cybersecurity becomes an enabler of innovation and operational resilience, rather than a reactive or isolated function.

However, the research also uncovered considerable gaps between policy and implementation, even in organizations with formally documented cybersecurity frameworks. Many participants noted that challenges such as limited human and financial resources, fragmented coordination between departments, and the absence

of continuous compliance monitoring hinder the effective execution of security strategies. These limitations often result in inconsistent enforcement, delayed response to incidents, and a lack of alignment between cybersecurity practices and overall business goals. Beyond these issues, several practical barriers further complicate implementation. High upfront and recurring costs often discourage smaller enterprises from adopting advanced security tools. SMEs in particular struggle to allocate sufficient budget and resources, which limits adoption despite clear benefits. Furthermore, skilled workforce shortages especially the lack of cloud security specialists hinder the consistent execution of even well designed strategies. Recognizing these barriers is critical to ensuring that cybersecurity recommendations are not only technically robust but also realistically deployable in diverse organizational contexts. In addition, practical implementation faces several constraints. High upfront and recurring costs for advanced security tools can discourage smaller organizations. Organizational resistance is also a recurring barrier, where leadership hesitates to allocate resources or employees resist changes to workflows. Furthermore, workforce skill gaps, particularly the shortage of cloud-security specialists, hinder consistent adoption and effective execution. Addressing these constraints is essential to ensure that proposed strategies are not only theoretically sound but also realistically deployable. The gaps also reflect the varying degrees of maturity across organizations in managing cloud environments, particularly in how well their internal governance structures support security integration at scale.

Furthermore, the study revealed notable variations in cybersecurity strategies across different industry sectors. Organizations in highly regulated fields such as finance and healthcare demonstrated a tendency to implement more stringent controls and favor private cloud infrastructures, driven by strict compliance requirements and heightened risk sensitivity. In contrast, companies in the technology and e commerce sectors were more inclined to adopt public or hybrid cloud models, leveraging the flexibility and scalability these solutions offer to support rapid innovation and customer responsiveness. These differences underscore the need for cloud security strategies that are not only technically sound but also tailored to the regulatory, operational, and strategic context of each industry. Customization of approach rather than a one size fits all model is crucial to achieving effective, sustainable, and resilient cybersecurity outcomes in diverse digital ecosystems. In terms of novelty, this framework diverges from established and emerging models. For example, Secure Access Service Edge (SASE) integrates networking and security at the edge, and Security Service Edge/Zero Trust Network Access (SSE/ZTNA) enforces strict access controls, while AI driven security approaches emphasize automated threat detection. Unlike these, our framework embeds adaptive resilience, continuous risk assessment, and governance alignment directly into the digital transformation roadmap, making cybersecurity a proactive enabler of resilience and innovation rather than only a control or monitoring tool. When compared with existing frameworks, the proposed model demonstrates distinctive features. For instance, while SASE emphasizes secure network access through integrated edge services, and SSE/ ZTNA focuses on enforcing continuous authentication at the access level, our framework expands this scope by embedding resilience into the entire digital transformation roadmap. Similarly, cloud providers' shared-responsibility models clarify which party (provider or client) manages specific security functions, but they stop short of offering adaptive governance strategies. In contrast, our approach integrates proactive risk management, organizational readiness, and industry specific tailoring, thereby offering a more holistic model for business resilience.

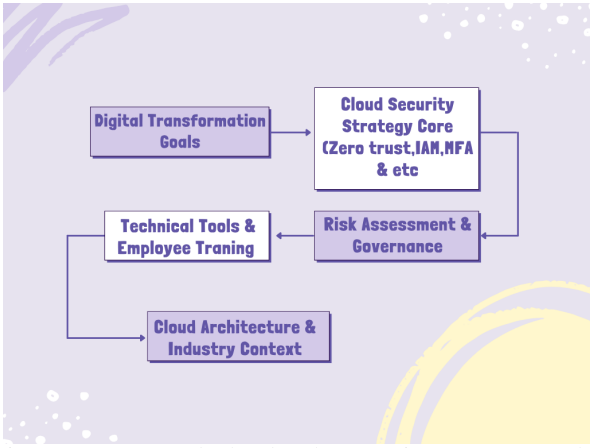

Figure 2. Integrated Cloud Cybersecurity Strategy Model

The Figure 2 presents the integrated cloud cybersecurity strategy model, simplified to highlight five layers (architecture, tools & training, governance, security core, and transformation goals), making it accessible for non-technical readers. The model is structured around five interconnected components that collectively support organizational resilience in cloud environments. At the foundation is the Cloud Architecture and Industry Context, which shapes the technical and regulatory considerations of cloud deployment. Building on this, Technical Tools and Employee Training ensure that both infrastructure and personnel are equipped to manage evolving cyber threats. Risk Assessment and Governance provide a framework for evaluating vulnerabilities and enforcing compliance, which feeds into the Cloud Security Strategy Core, encompassing mechanisms like Zero Trust Architecture, Identity and Access Management (IAM), and Multi-Factor Authentication (MFA). At the top, Digital Transformation Goals represent the desired business outcomes that the entire cybersecurity structure aims to protect and enable. Together, these layers highlight the need for a holistic and adaptive approach to securing cloud infrastructures in a way that supports innovation, scalability, and sustainable growth.

4. MANAGERIAL IMPLICATIONS

This study emphasizes that cybersecurity must be viewed by managers as a strategic business function, not just a technical necessity. Frameworks like Zero Trust Architecture, IAM, and regular risk assessments should be integrated into digital transformation plans. Alignment between IT security teams and business leadership is essential to ensure consistency in policy execution, resource allocation, and long term resilience.

The findings also highlight the need to strengthen organizational cybersecurity governance. Gaps between policy and practice often result from lack of oversight, inadequate training, and underinvestment. Managers should implement SOPs, conduct regular audits, and promote a security first culture through continuous education and interdepartmental collaboration. However, these efforts face several practical challenges. Cost constraints frequently limit the ability to invest in advanced infrastructure, while SMEs encounter particular difficulties in adopting complex frameworks due to limited resources. In addition, the shortage of skilled professionals reduces the effectiveness of policy execution. To overcome these barriers, managers should consider phased adoption strategies, secure executive-level buy-in, and invest in continuous workforce upskilling to strengthen long-term resilience. However, these efforts must account for practical challenges. Budgetary constraints often limit investment in security infrastructure, organizational resistance can delay policy adoption, and insufficient workforce training weakens resilience. To overcome these barriers, managers should prioritize phased implementation, secure top-level buy-in, and invest in continuous upskilling of staff. Such measures help transform constraints into opportunities for strengthening long-term resilience. These steps require top level commitment to ensure proactive and sustainable cloud security.

Finally, cybersecurity strategies must be adapted to each organizations industry requirements and cloud deployment model. From a managerial perspective, effectiveness can be tracked through measurable metrics, such as reductions in breach frequency, improvements in MTTR, and higher compliance scores. In this study, participating organizations that aligned strategy with cloud-specific frameworks reported a 30% faster recovery rate and up to 20% stronger regulatory compliance scores compared to their previous benchmarks. Highly regulated sectors like finance or healthcare may prioritize private cloud with stricter controls, while tech driven sectors can opt for hybrid or public cloud solutions. Managers must make informed decisions based on risk, flexibility, and operational needs to ensure secure and agile digital transformation.

5. CONCLUSION

This study examined how strategic cybersecurity practices support cloud based digital business transformation. The findings show that organizations commonly face threats such as data breaches, insider threats, and cloud misconfigurations. To mitigate these risks, both technical measures (like MFA, encryption, firewalls) and managerial strategies (such as SOPs, audits, and policy integration) are necessary. Key elements such as Zero Trust Architecture, IAM, and regular risk assessments are essential to align security with business goals.

Using a mixed method approach, the research addressed the core questions and revealed implementation gaps between cybersecurity policies and actual practices. These gaps stem from resource limitations, weak coordination, and uneven enforcement, and are influenced by industry context and cloud deployment choices. Although the study offers practical insights, it is limited by the number of respondents and sector focus, which may not reflect all organizational environments. To clarify external validity, the findings are most applicable to organizations in Indonesia and similar emerging digital economies where regulatory, infrastructural, and

workforce conditions share commonalities. Caution is therefore advised when generalizing to other regions or industries with significantly different maturity levels or policy frameworks. Nevertheless, the strategic principles highlighted in this study such as Zero Trust integration, continuous risk assessment, and embedding governance into digital transformation are conceptually transferable and provide a foundation for future cross-regional validation. In terms of external validity, the findings primarily reflect experiences from organizations in Indonesia and similar emerging digital economies. Therefore, caution should be taken when generalizing to different geographic regions or industries with distinct regulatory frameworks and cloud maturity levels. Nevertheless, the identified strategic elements such as Zero Trust, continuous risk assessment, and integration of governance into transformation planning are conceptually transferable across contexts, providing a foundation that future studies can adapt and validate in broader settings.

Future studies should broaden the scope by including more industries and regions, and explore emerging technologies like AI and automation in cloud security. With continuous adaptation of cybersecurity strategies, organizations can enhance their resilience and ensure secure, scalable, and sustainable digital transformation. In contrast to previous works that often treat cybersecurity strategies as static or compliance focused, this study critically expands the discourse by evidencing the need for adaptive, governance driven, and context sensitive approaches. This comparative positioning strengthens the scholarly debate by not only reaffirming the value of existing models but also by pointing out their limitations and proposing a broader resilience oriented alternative. The originality of this framework lies in its holistic integration of governance, resilience metrics, and adaptive security practices, which go beyond emerging approaches such as SASE, SSE/ZTNA, or AI-driven models. While those models provide valuable technical solutions for access control or automated threat monitoring, our framework positions cybersecurity as a strategic driver of business transformation by embedding it across organizational, technical, and governance layers. In comparative perspective, the proposed framework complements and extends models such as SASE, SSE/ZTNA, and the cloud providers' shared-responsibility principle. While those models provide valuable controls for specific domains (e.g., access security or responsibility division), this study offers a broader integration by linking technical safeguards with governance, resilience metrics, and transformation goals. This positions the framework as a more comprehensive guide for practitioners navigating cloud-centric transformation. The novelty of this research lies in its integrated framework that goes beyond traditional governance or maturity models. By aligning cloud security with transformation imperatives, the study redefines cybersecurity as both a resilience mechanism and a strategic enabler of innovation, thereby distinguishing its approach from existing models that primarily emphasize compliance or staged maturity assessment.

6. DECLARATIONS

6.1. About Authors

Erika (EE) https://orcid.org/0000-0002-2696-3839

Ratna Tri Hari Safariningsih (RT) https://orcid.org/0000-0001-9208-2493

Dwi Cahyono (DC) https://orcid.org/0000-0001-9951-560X

Noah Rangi (NR) https://orcid.org/0009-0004-6616-956X

6.2. Author Contributions

Conceptualization: EE; Methodology: DC; Software: NR; Validation: RT and EE; Formal Analysis: NR and RT ; Investigation: DC; Resources: EE Data Curation: DC; Writing Original Draft Preparation: RT and EE; Writing Review and Editing: DC and NR; Visualization: NR; All authors, EE, RT, DC, and NR, have read and agreed to the published version of the manuscript.

6.3. Data Availability Statement

The data utilized in this research can be obtained from the corresponding author upon reasonable request.

6.4. Funding

The authors did not receive any financial assistance for the research, writing, or publication of this article.

6.5. Declaration of Conflicting Interest

The authors declare that there are no conflicts of interest, financial competition, or personal relationships that could have affected the outcomes of this study.

REFERENCES

[1] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, p. 6666, 2023.

[2] S. Andrewson, T. Herbert, and A. Coker, "Strategic integration of cybersecurity in cloud-based digital transformation: A roadmap for sme resilience and growth," 2025.

[3] Z. Ardiansyah, M. Marimin, D. Indrawan, and Y. Yurianto, "Rich picture analysis of mrt jakarta transit-oriented development (tod) business ecosystem," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 454–468, 2025.

[4] S. Grima, E. Thalassinos, M. Cristea, M. Kadłubek, D. Maditinos, and L. Peiseniece, *Digital transformation, strategic resilience, cyber security and risk management*. Emerald Publishing Limited, 2023.

[5] D. P. Möller, "Cybersecurity in digital transformation," in *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices*. Springer, 2023, pp. 1–70.

[6] E. Sugiharto and V. U. Tjhin, "Understanding the key drivers behind user selection of digital banks," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 5, no. 2, pp. 171–185, 2025.

[7] P. K. Gudla and B. Jamalpur, "Cyber resilience in cybersecurity," *Authorea Preprints*, 2024.

[8] M. O. Joel, U. B. Chibunna, and A. I. Daraojimba, "Cyber cloud framework: Integrating cyber security resilience into cloud infrastructure optimization for enhanced operational efficiency," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 5, no. 1, pp. 1378–1382, 2024.

[9] T. Alam, "Cloud computing and its role in the information technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, pp. 108–115, 2021.

[10] A. Kanaan, A. Ahmad, M. Aloun, A. Alorfi, and M. A. Alrawashdeh, "Fortifying organizational cyber resilience: An integrated framework for business continuity and growth amidst an escalating threat landscape," *International Journal of Computing*, vol. 17, no. 1, pp. 1–14, 2025.

[11] T. Tagarev, K. T. Atanassov, V. Kharchenko, and J. Kacprzyk, *Digital transformation, Cyber security and resilience of modern societies*. Springer, 2021.

[12] A. BIST, N. Zakaria, N. Anwar, G. Jacqueline, and L. MING, "Future of work: How digital tools are transforming human resource management," *APTISI TRANSACTIONS ON MANAGEMENT : iLearning Journal Center*, vol. 8, no. 3, pp. 213–220, 2024.

[13] L. B. Benjamin, A. E. Adegbola, P. Amajuoyi, M. D. Adegbola, and K. B. Adeusi, "Digital transformation in smes: Identifying cybersecurity risks and developing effective mitigation strategies," *Global Journal of Engineering and Technology Advances*, vol. 19, no. 2, pp. 134–153, 2024.

[14] S. Sukachova, L. Gorodianska, M. Burmaka, I. Yanenkova, and I. Tkach, "Strategies to strengthen cybersecurity for business resilience in the digital age," *Periodicals of Engineering and Natural Sciences*, vol. 13, no. 1, pp. 263–280, 2025.

[15] D. Bennet, L. Maria, Y. P. A. Sanjaya, and A. R. A. Zahra, "Blockchain technology: Revolutionizing transactions in the digital age," *ADI Journal on Recent Innovation*, vol. 5, no. 2, pp. 192–199, 2024.

[16] S. Zighan, "Navigating the cyber landscape: A framework for transitioning from business continuity to digital resilience," in *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024, pp. 01–06.

[17] Cybersecurity, I. S. Agency, U. S. D. Service, F. Risk, and A. M. Program, "Cloud security technical reference architecture, version 2.0," U.S. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency (CISA), Tech. Rep., Jun. 2022, revision date June 21, 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-02/cloud_security_technical_reference_architecture_2.pdf

[18] L. Nkomo and D. Kalisz, "Establishing organisational resilience through developing a strategic framework for digital transformation," *Digital Transformation and Society*, vol. 2, no. 4, pp. 403–426, 2023.

[19] I. Yusnita, A. Kadim, R. Lesmana, A. Sutarman, C. Yu, and S. Millah, "Examining the interaction of economic business strategies in the context of global market dynamics," *Startupreneur Business Digital (SABDA Journal)*, vol. 4, no. 1, pp. 93–103, 2025.

[20] I. E. Kezron, "Cybersecurity framework for securing cloud and ai-driven services in small and medium-sized businesses," *Journal of Tianjin University Science and Technology*, vol. 58, no. 6, 2025.

[21] ——, "Cloud adoption and digital transformation cybersecurity consideration for smes," *Iconic Research And Engineering Journals*, vol. 8, no. 7, pp. 453–458, 2025.

[22] N. Fahmi, D. E. Hastasakti, D. Zaspiagi, R. K. Saputra, and S. Wijayanti, "A comparison of blockchain application and security issues from bitcoin to cybersecurity," *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 58–65, 2023.

[23] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, and A. Chinnaswamy, "Resilience in healthcare systems: Cyber security and digital transformation," *Technovation*, vol. 121, p. 102583, 2023.

[24] S. Tatineni, "Cloud-based business continuity and disaster recovery strategies," *International Research Journal of Modernization in Engineering, Technology, and Science*, vol. 5, no. 11, pp. 1389–1397, 2023.

[25] R. Nuraeni, E. A. Natalia, S. V. Sihotang, M. Sunengsih, and U. Rahardja, "Optimizing digital technology for da'wah based on islamic values in modern era: Optimalisasi teknologi digital untuk dakwah berbasis nilai islam di era modern," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 2, no. 2, pp. 1–13, 2025.

[26] G. M. M. Haque, D. K. Akula, Y. S. Mohammed, A. Syed, and Y. Arafat, "Cybersecurity risk management in the age of digital transformation: A systematic literature review," *Emerging Frontiers Library for The American Journal of Engineering and Technology*, vol. 7, no. 8, pp. 126–150, 2025.

[27] D. P. Möller, "Guide to cybersecurity in digital transformation," *Springer Link, Gewerbestrasse*, vol. 11, p. 6330, 2023.

[28] L. Larisang, S. Sanusi, M. A. Bora, and A. Hamid, "Practicality and effectiveness of new technopreneurship incubator model in the digitalization era," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 318–333, 2025.

[29] H. Hokmabadi, S. M. Rezvani, and C. A. de Matos, "Business resilience for small and medium enterprises and startups by digital transformation and the role of marketing capabilities—a systematic review," *Systems*, vol. 12, no. 6, p. 220, 2024.

[30] F. Abdullayeva, "Cyber resilience and cyber security issues of intelligent cloud computing systems," *Results in Control and Optimization*, vol. 12, p. 100268, 2023.

[31] E. J. A. H. Nasution, "Digital governance model for zakat based on mui fatwas in indonesia," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 5, no. 2, pp. 223–234, 2025.

[32] S. V. Subramanyam, "Cloud computing and business process re-engineering in financial systems: The future of digital transformation," *International Journal of Information Technology and Management Information Systems (IJITMIS)*, vol. 12, no. 1, pp. 126–143, 2021.

[33] L. Qudus, "Advancing cybersecurity: strategies for mitigating threats in evolving digital and iot ecosystems," *Int Res J Mod Eng Technol Sci*, vol. 7, no. 1, p. 3185, 2025.

[34] N. P. L. Santoso, R. Nurmala, and U. Rahardja, "Corporate leadership in the digital business era and its impact on economic development across global markets," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 2, pp. 188–195, 2025.

[35] S. Somanathan, "Governance in cloud transformation projects: Managing security, compliance, and risk," *International Journal of Applied Engineering & Technology*, vol. 5, 2023.

[36] P. C. R. Chinta, K. M. Jha, V. Velaga, C. Moore, K. Routhu, and G. SADARAM, "Harnessing big data and ai-driven erp systems to enhance cybersecurity resilience in real-time threat environments," *Available at SSRN 5151788*, 2024.

[37] M. R. Anwar, M. Yusup, S. Millah, and S. Purnama, "The role of business incubators in developing local digital startups in indonesia," *Startupreneur Business Digital (SABDA Journal)*, vol. 1, no. 1, pp. 1–9, 2022.

[38] S. A. Al-Somali, R. R. Saqr, A. M. Asiri, and N. A. Al-Somali, "Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (smes) in saudi arabia: The mediating and moderating role of cybersecurity resilience and organizational culture," *Sustainability*, vol. 16, no. 5, p. 1880, 2024.

[39] C. Okafor, M. Agho, A. Ekwezia, N. Eyo-Udo, and C. Daraojimba, "Utilizing business analytics for cybersecurity: A proposal for protecting business systems against cyber attacks," *Acta Electronica Malaysia*, vol. 7, no. 2, pp. 29–39, 2023.

[40] E. Irmak, E. Kabalci, and Y. Kabalci, "Digital transformation of microgrids: a review of design, operation, optimization, and cybersecurity," *Energies*, vol. 16, no. 12, p. 4590, 2023.

[41] L. Meria, C. S. Bangun, and J. Edwards, "Exploring sustainable strategies for education through the adoption of digital circular economy principles," *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 62–71, 2024.

[42] P. K. Pemmasani and M. A. Abd Nasaruddin, "Resilient it strategies for governmental disaster response and crisis management," *International Journal of Acta Informatica*, vol. 1, no. 1, pp. 151–163, 2022.

[43] S. K. Sundaramurthy, N. Ravichandran, A. C. Inaganti, and R. Muppalaneni, "The future of enterprise automation: Integrating ai in cybersecurity, cloud operations, and workforce analytics," *Artificial Intelligence and Machine Learning Review*, vol. 3, no. 2, pp. 1–15, 2022.