The Eastasouth Journal of Information System and Computer Science
Vol. 3, No. 02, December 2025, pp. 227-241
ISSN: 3025-566X, DOI: 10.58812/esiscs.v3i02

Improving Cybersecurity Resilience in Indonesian Cloud Infrastructures Through AI-Based Threat Intelligence

Manase Sahat H Simarangkir
Politeknik Meta Industri Cikarang

Article Info

Article history:

Received Dec, 2025
Revised Dec, 2025
Accepted Dec, 2025

Keywords:

Artificial Intelligence;
Cloud Infrastructure;
Cybersecurity Resilience;
SEM-PLS;
Threat Intelligence

ABSTRACT

The rapid expansion of cloud computing adoption in Indonesia has significantly increased organizational exposure to cyber threats, making cybersecurity resilience a critical strategic priority. This study examines the role of Artificial Intelligence (AI)-based threat intelligence in enhancing cybersecurity resilience within Indonesian cloud infrastructure. Using a quantitative research design, data were collected from 155 respondents consisting of IT managers, cloud engineers, and cybersecurity practitioners through a structured Likert-scale questionnaire. The data were analyzed using Structural Equation Modeling–Partial Least Squares (SEM-PLS 3). The results indicate that AI-based threat intelligence has a significant positive effect on threat detection accuracy and response effectiveness. Both threat detection accuracy and response effectiveness also have significant positive effects on cybersecurity resilience. Furthermore, AI-based threat intelligence directly strengthens cybersecurity resilience and indirectly enhances it through the mediation of threat detection accuracy and response effectiveness. These findings confirm that AI-driven cybersecurity systems play a strategic role in improving adaptive defense capabilities, accelerating incident response, and strengthening organizational resilience in cloud environments. This study provides important implications for policymakers, cloud service providers, and organizations in designing intelligent cybersecurity frameworks to support Indonesia's sustainable digital transformation.

Corresponding Author:

Name: Manase Sahat H Simarangkir
Institution: Politeknik Meta Industri Cikarang
Email: manasemalo@politeknikmeta.ac.id

1. INTRODUCTION

The rapid acceleration of digital transformation in Indonesia has significantly intensified the adoption of cloud computing across government institutions, financial sectors, startups, and large enterprises, driven by the need for scalability, cost efficiency, and operational agility as essential components of the nation's digital economy roadmap; however, this expansion simultaneously exposes critical digital assets to increasingly sophisticated cyber threats such as ransomware, data breaches, distributed denial-of-service (DDoS), phishing, and advanced persistent threats (APTs), making cybersecurity resilience a strategic imperative rather than a technical option. The integration of multi-cloud architectures further elevates system complexity and creates new vulnerabilities, including data breaches and identity management issues [1], while the intricate structure of cloud environments

demands advanced and adaptive security frameworks [2]. To address these risks, organizations must implement Zero Trust Architecture, end-to-end data encryption, and automated security policy enforcement as effective mitigation strategies in multi-cloud ecosystems [1], supported by proactive and multilayered cybersecurity frameworks to reduce system vulnerabilities and maintain robust protection [1]. In the government sector, cloud adoption continues to face challenges related to data security, budget constraints, and limited strategic vision among leadership [3], [4], further exacerbated by rigid institutional structures and digital skill gaps [5], Strengthening cybersecurity infrastructure and improving digital literacy therefore become critical factors for overcoming these challenges and establishing a resilient digital defense [6], while engaging all stakeholders and ensuring supportive regulatory ecosystems are essential for successful digital transformation [6].

Cybersecurity resilience refers to an organization's ability to anticipate, withstand, recover from, and adapt to cyber incidents while maintaining continuity of operations, and in cloud environments this resilience becomes even more critical due to the shared responsibility model, dynamic resource allocation, and the high interconnectivity of systems; however, traditional security approaches that depend on static rule-based detection and perimeter defense are no longer sufficient to address rapidly evolving threats and zero-day vulnerabilities, creating a substantial gap between emerging risks and the capabilities of conventional cloud security systems. In this context, Artificial Intelligence (AI) has emerged as a transformative enabler of AI-based threat intelligence systems that leverage machine learning, deep learning, and big data analytics to detect anomalous behavior, predict attack patterns, automate threat classification, and support real-time cyber incident responses, operating dynamically by continuously learning from massive volumes of threat data and enabling proactive rather than reactive defense strategies—an ability that is essential in cloud ecosystems with high traffic, diverse access points, and constantly evolving threat vectors. AI-based threat intelligence systems therefore play a critical role in strengthening cybersecurity resilience by detecting, predicting, and responding to cyber threats more effectively than traditional tools, with dynamic learning capabilities that ensure continuity of operations even during sophisticated attacks, supported by evidence showing significantly improved detection accuracy and faster response times through real-time analysis of large-scale data, anomaly identification, and attack pattern prediction [7], [8], including demonstrated detection accuracy rates of up to 98.5% and reductions in false positives and false negatives [9], while automated response mechanisms further enhance proactive defense by minimizing mitigation time [10]. Moreover, AI's adaptability and continuous learning allow systems to respond to emerging threats in dynamic cloud settings [7], [10], with supervised and unsupervised models such as Random Forest and Isolation Forest improving the classification of known threats and detection of new anomalies [10]. Despite these advantages, challenges persist—including data privacy concerns, the need for high-quality training datasets, and vulnerability to adversarial attacks [7], [11] highlighting the need for ongoing research to enhance model interpretability and integrate AI technologies effectively into existing security infrastructures to maximize their impact [11], [12].

In the Indonesian context, the challenge of cybersecurity resilience is compounded by disparities in cybersecurity maturity, limited skilled professionals, uneven adoption of advanced security technologies, and inconsistent regulatory compliance; despite strengthened government efforts in national cybersecurity governance, many organizations—especially SMEs—remain vulnerable to cyber disruptions. Integrating AI-based threat intelligence into cloud security architectures offers a critical opportunity to enhance national cyber resilience by addressing maturity gaps, skill shortages, and uneven technology adoption while improving

detection, response, and cross-sector collaboration essential for protecting critical information infrastructure [13]. However, successful AI implementation must overcome governance and regulatory barriers and requires stronger organizational resilience supported by strategic digital transformation and leadership commitment [14], [15]. Key challenges include limited leadership support and resource constraints that hinder effective cybersecurity governance [14], as highlighted by the Global Cybersecurity Index indicating Indonesia's low commitment and maturity [16]. The shortage of skilled professionals reinforces the need for investment in training and capacity building across sectors (S et al., 2024), with human capital development essential for leveraging AI technologies effectively [13]. Although uneven adoption of advanced security technologies persists, AI can accelerate adoption through improved threat detection and response [13], while strategic digital transformation strengthens organizational preparedness [15]. Moreover, varying levels of regulatory compliance and insufficient legal frameworks continue to hinder readiness [17], and AI deployment must address risks such as privacy violations and data leaks, requiring strict adherence to regulatory standards [13].

Despite the growing global discourse on AI in cybersecurity, empirical studies that quantitatively examine the impact of AI-based threat intelligence on cybersecurity resilience in cloud environments—particularly within developing digital economies such as Indonesia—remain limited, as most existing studies focus on conceptual frameworks, technical algorithm performance, or case-based system implementations, leaving a gap in robust statistical evidence explaining how AI-based threat intelligence influences key cybersecurity outcomes such as threat detection accuracy, response effectiveness, and organizational-level resilience. This study addresses this research gap by empirically investigating the effect of AI-based threat intelligence on cybersecurity resilience in Indonesian cloud infrastructure through a quantitative approach using data from 155 respondents, including cloud system users, IT managers, and cybersecurity practitioners, collected via structured Likert-scale instruments, with the relationships among AI-based threat intelligence, threat detection accuracy, response effectiveness, and cybersecurity resilience analyzed using Structural Equation Modeling–Partial Least Squares (SEM-PLS 3), enabling simultaneous testing of complex causal relationships between latent variables. The findings of this study are expected to contribute both theoretically and practically by enriching the cybersecurity and information systems literature through empirical validation of AI-driven security frameworks in cloud environments and by offering strategic insights for policymakers, cloud service providers, and organizational leaders in designing AI-enabled cybersecurity architectures that strengthen resilience against evolving cyber threats, ultimately supporting Indonesia's digital transformation agenda by emphasizing that technological advancement must be accompanied by robust, intelligent, and adaptive cybersecurity systems.

2. LITERATURE REVIEW

2.1 Cybersecurity Resilience in Cloud Infrastructure

Cybersecurity resilience in cloud environments is increasingly critical as organizations face sophisticated threats and complex infrastructures, shifting the focus from prevention toward the ability to anticipate, withstand, respond to, recover from, and adapt to cyberattacks while maintaining operational continuity, particularly in multi-tenant cloud ecosystems where shared responsibility models introduce unique vulnerabilities. While resilient frameworks traditionally integrate layered protection strategies, the dynamic nature of modern cyber threats requires adaptive and intelligent systems capable of real-time learning and response; next-generation frameworks therefore emphasize AI-driven threat detection, automated recovery, and continuous monitoring, demonstrating significant improvements in recovery

time and detection accuracy for critical sectors such as healthcare and finance [18]. However, challenges intensify in multi-cloud environments where discrete security systems expand attack vectors, necessitating innovative security models such as Zero Trust Architecture (ZTA) and Identity-Based Access Control (IBAC) to mitigate inter-cloud communication risks [19]. AI-driven Cloud Security Posture Management (CSPM) frameworks further enhance resilience by leveraging machine learning and intelligent automation to proactively analyze network interactions, predict vulnerabilities, and enable rapid, context-aware responses [20]. Despite these advancements, scalability limitations, integration barriers, and resource constraints continue to hinder widespread adoption of resilient frameworks [19], underscoring that cybersecurity resilience is not merely a technical requirement but a strategic imperative affecting business continuity, organizational reputation, and regulatory compliance [12], [21].

2.2 *Artificial Intelligence-Based Threat Intelligence*

Artificial Intelligence (AI) has significantly transformed cybersecurity by enhancing large-scale data processing, complex pattern recognition, and predictive threat analysis, with AI-based threat intelligence systems leveraging machine learning, deep learning, natural language processing, and big data analytics to autonomously collect and interpret threat information for proactive security decision-making. Unlike traditional approaches, AI continuously learns from diverse data sources to detect anomalies, classify threats, and prioritize responses in real time, supporting critical functions such as intrusion detection, malware classification, phishing prevention, and automated incident response. Empirical evidence shows that AI-powered systems achieve higher detection rates (92.3% vs. 78.5%), lower false positives (8.7% vs. 15.2%), and faster response times (15.2s vs. 45.0s) [22], while machine learning and deep learning techniques—including convolutional and recurrent neural networks—demonstrate superior performance in detecting complex threats [23], and AI integration reduces response time by up to 45% while improving accuracy [24]. Techniques such as Random Forest and Support Vector Machine models also enhance detection accuracy by 17–35% [24], with NLP improving phishing detection and log analysis, and reinforcement learning enabling adaptive incident response. Despite these advancements, AI-based cybersecurity faces challenges related to data quality, algorithmic bias, adversarial attacks, and high computational demands [25], [26], while ethical concerns regarding bias and accountability underscore the need for transparency in AI deployment [25].

2.3 *Threat Detection Accuracy*

AI-based threat detection systems significantly enhance detection accuracy in cloud environments by using machine learning and deep learning models to identify complex patterns and behavioral anomalies that traditional signature-based systems often miss, making them highly effective in addressing challenges such as high data velocity, encrypted traffic, and decentralized architectures. By learning behavioral profiles, AI models can more accurately detect polymorphic malware, zero-day exploits, and stealthy attacks, thereby strengthening incident response and long-term cybersecurity resilience. Empirical evidence shows that AI-powered systems achieve superior performance, with detection accuracy reaching 98.5% and reduced false negative and false positive rates of 2.0% and 1.2%, respectively [9], and the ability to detect up to 320 threats per day—far exceeding traditional systems [22]. These advantages are further reinforced by real-time data analysis capabilities essential in high-velocity cloud environments [8] and by continuous model training that

enhances adaptability to emerging threats [27]. Additionally, AI-driven detection significantly reduces false positives through advanced anomaly detection algorithms, improving reliability and minimizing alert fatigue among security teams [28].

2.4 *Response Effectiveness in Cybersecurity*

AI-based threat intelligence significantly enhances response effectiveness in cloud environments by automating and accelerating the detection and mitigation of cyber threats, addressing the limitations of traditional incident response frameworks that rely on human intervention and cannot match the rapid propagation of attacks across interconnected systems. AI enables real-time anomaly detection and threat pattern analysis, substantially reducing mean time to detect (MTTD) and mean time to respond (MTTR) [8], [29], while machine learning models such as Random Forest achieve high threat-classification accuracy, including up to 96% in malware analysis [30]. Furthermore, AI-driven systems can autonomously initiate remediation actions—such as blocking malicious IPs and isolating infected virtual machines—without human input [29], [31], and can dynamically identify and eliminate new threats with false negative and false positive rates as low as 2.0% and 1.2% [9]. Continuous learning enables these systems to refine response strategies and adapt to evolving threat landscapes [8], [29], thereby strengthening long-term cybersecurity resilience [8].

2.5 *Research Gap and Conceptual Framework Development*

Although existing studies have widely explored the technical capabilities of AI in cybersecurity, limited empirical research has quantitatively examined how AI-based threat intelligence influences cybersecurity resilience through intermediate operational mechanisms such as threat detection accuracy and response effectiveness, particularly within emerging digital economies like Indonesia. Prior research largely emphasizes system-level performance tests, algorithmic comparisons, and qualitative risk assessments, leaving a notable gap in statistical validation of AI-driven cybersecurity models at the organizational level, especially studies that integrate detection accuracy and response effectiveness as mediating variables. To address this gap, the present study proposes a conceptual framework in which AI-based threat intelligence directly enhances cybersecurity resilience and indirectly strengthens it through improved detection accuracy and response effectiveness, and this framework is empirically tested using SEM-PLS 3 to provide robust evidence on the structural relationships among these constructs within Indonesia's cloud infrastructure landscape.

3. RESEARCH METHODS

3.1 *Research Design*

This study adopts a quantitative research design with a causal–explanatory approach to examine the effect of Artificial Intelligence (AI)-based threat intelligence on cybersecurity resilience in Indonesian cloud infrastructure. The quantitative approach is appropriate because this research aims to test hypothesized relationships among latent variables using statistical modeling. The study employs Structural Equation Modeling–Partial Least Squares (SEM-PLS 3) as the primary analytical technique due to its suitability for predictive research, complex models, and relatively moderate sample sizes. The research model is designed to explain the direct and indirect effects of AI-based threat intelligence on cybersecurity resilience, with threat detection accuracy and response effectiveness acting as mediating variables. This design enables comprehensive testing of both structural and measurement models simultaneously.

3.2 Population and Sample

The population of this study consists of individuals directly involved in or knowledgeable about cloud computing and cybersecurity practices in Indonesia, including IT managers and system administrators, cybersecurity professionals, cloud infrastructure engineers, cloud service users with security responsibilities, and digital transformation officers or IT consultants. A total of 155 respondents were selected using purposive sampling, requiring participants to meet specific criteria related to experience in cloud infrastructure usage and cybersecurity management to ensure that the data collected were relevant, valid, and aligned with the research objectives. The sample size of 155 is considered adequate for SEM-PLS analysis, which is robust for small to medium samples and well suited for predictive modeling.

3.3 Data Collection Method

Primary data were collected using a structured questionnaire distributed online to respondents across various regions in Indonesia. The questionnaire was developed based on an extensive literature review and adapted to the Indonesian cloud infrastructure context. All measurement items were rated using a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree) and covered four main constructs: AI-Based Threat Intelligence (AITI), Threat Detection Accuracy (TDA), Response Effectiveness (RE), and Cybersecurity Resilience (CR). To ensure clarity and content validity, a pilot test was conducted with a small group of respondents before the full data collection process, and the feedback obtained was used to refine ambiguous statements and enhance instrument reliability.

The operational definitions of the variables include: (1) AI-Based Threat Intelligence (AITI), defined as the organization's capability to use AI technologies to collect, analyze, and interpret cyber threat data, measured through indicators such as automated large-scale data analysis, real-time anomaly detection, predictive threat analytics, automated threat classification, and integration with security monitoring systems; (2) Threat Detection Accuracy (TDA), referring to the ability of cybersecurity systems to correctly identify malicious activities while minimizing false positives and false negatives, with indicators including accurate threat identification, low false alarm rates, detection of unknown attacks, timely detection, and reliable outcomes; (3) Response Effectiveness (RE), which denotes the efficiency and precision of actions taken to mitigate cyber threats once detected, measured through indicators such as response speed, containment effectiveness, automation of response processes, accuracy of mitigation actions, and rapid system recovery; and (4) Cybersecurity Resilience (CR), defined as an organization's ability to anticipate, withstand, recover from, and adapt to cyber incidents while maintaining operational continuity, reflected in indicators including service continuity during attacks, recovery speed, adaptive system improvement, organizational preparedness, and reliability of cloud operations.

3.4 Data Analysis Technique

The collected data were analyzed using SEM-PLS 3, a method suitable for complex causal modeling that does not require strict normality assumptions, and the analysis consisted of two main stages: the measurement model (outer model) evaluation and the structural model (inner model) evaluation. The outer model assessment examined instrument validity and reliability through convergent validity (outer loadings > 0.70 and AVE > 0.50), discriminant validity using the Fornell–Larcker Criterion and cross-loadings, and reliability through Composite Reliability and Cronbach's Alpha (both > 0.70). The inner model evaluation analyzed the structural

relationships among latent variables using path coefficients, coefficient of determination (R^2) for explanatory power, predictive relevance (Q^2), and effect size (f^2), while hypothesis testing was conducted through bootstrapping with 5,000 resamples to determine the significance of all proposed relationships.

4. RESULTS AND DISCUSSION

4.1 Respondent Profile Overview

This study involved 155 respondents selected based on their active involvement and experience in cloud infrastructure management and cybersecurity implementation in Indonesia, ensuring that the data reflected informed professional perspectives relevant to evaluating the role of AI-based threat intelligence in strengthening cybersecurity resilience. The respondent profile was dominated by IT managers, system administrators, cybersecurity analysts, and cloud engineers, with additional representation from digital transformation officers, IT consultants, and cloud security supervisors—indicating that most participants occupied strategic or technical roles directly related to cybersecurity decision-making and operational execution. In terms of professional experience, the majority had more than three years of experience, with a substantial portion exceeding five years, reflecting mature familiarity with cloud risks, security procedures, and incident response challenges, while early-career professionals with one to three years of experience contributed additional operational insights. Respondents also represented diverse organizational sectors, including government, financial services, telecommunications, education, e-commerce, manufacturing, and technology startups, demonstrating that cloud-security challenges span multiple industries across Indonesia's digital economy.

Furthermore, most respondents reported high levels of cloud usage within their organizations, including reliance on cloud services for data storage, application hosting, system integration, and digital service delivery, with many handling sensitive or mission-critical data such as financial records, personal information, and operational databases—reinforcing the importance of cybersecurity resilience as a strategic priority. The majority also indicated direct involvement in cybersecurity operations, including security monitoring, incident response, and risk management, ensuring that responses on AI-based threat intelligence, detection accuracy, response effectiveness, and cybersecurity resilience were grounded in practical experience rather than theoretical understanding. Overall, the respondent profile demonstrates that the sample is professionally mature, highly relevant, and sectorally diverse, thereby providing a strong empirical foundation for analyzing the impact of AI-based threat intelligence on cybersecurity resilience within Indonesia's cloud infrastructure landscape.

4.2 Measurement Model Evaluation (Outer Model)

The measurement model (outer model) evaluation was conducted to ensure that all constructs in this study satisfied the criteria for convergent validity, discriminant validity, and reliability, following SEM-PLS 3 standards using outer loading values, Average Variance Extracted (AVE), Composite Reliability (CR), and Cronbach's Alpha (CA). Convergent validity was confirmed through outer loading values exceeding 0.70 and AVE values above 0.50 for all indicators, demonstrating that each construct achieved strong validity and met the required measurement thresholds.

Table 1. Outer Loadings of Measurement Indicators

Construct	Indicator	Outer Loading
AI-Based Threat Intelligence (AITI)	AITI1	0.872
	AITI2	0.901
	AITI3	0.886
	AITI4	0.879
	AITI5	0.893
Threat Detection Accuracy (TDA)	TDA1	0.884
	TDA2	0.897
	TDA3	0.912
	TDA4	0.869
	TDA5	0.881
Response Effectiveness (RE)	RE1	0.891
	RE2	0.873
	RE3	0.902
	RE4	0.886
	RE5	0.879
Cybersecurity Resilience (CR)	CR1	0.895
	CR2	0.911
	CR3	0.887
	CR4	0.902
	CR5	0.884

Table 1 shows that all measurement indicators across the four constructs—AI-Based Threat Intelligence (AITI), Threat Detection Accuracy (TDA), Response Effectiveness (RE), and Cybersecurity Resilience (CR)—demonstrate strong convergent validity, as reflected in outer loading values exceeding the recommended threshold of 0.70. The AITI construct exhibits high loadings ranging from 0.872 to 0.901, indicating that each indicator consistently captures the underlying dimension of AI-driven threat intelligence capabilities. Similarly, the TDA construct records exceptionally strong loadings between 0.869 and 0.912, demonstrating that the indicators accurately represent system accuracy in identifying cyber threats. The RE construct also shows robust indicator performance with loading values between 0.873 and 0.902, confirming that the items effectively measure the efficiency and precision of organizational incident response mechanisms. Finally, the CR construct presents strong loadings from 0.884 to 0.911, suggesting that the indicators reliably capture the organization's capability to withstand, recover from, and adapt to cyber incidents. Overall, the consistently high outer loading values across all constructs provide compelling evidence that the measurement model demonstrates excellent convergent validity and that the indicators are both statistically sound and conceptually aligned with the theoretical constructs they are intended to measure.

Table results show that all constructs—AI-Based Threat Intelligence (AITI), Threat Detection Accuracy (TDA), Response Effectiveness (RE), and Cybersecurity Resilience (CR)—achieve strong Average Variance Extracted (AVE) values, ranging from 0.789 to 0.806. Since all AVE values exceed the recommended threshold of 0.50, this indicates that each construct successfully explains more than 50% of the variance of its measurement indicators. This also confirms strong convergent validity, meaning the indicators within each construct consistently measure the same underlying concept and provide reliable representation of the theoretical variables in the model.

Furthermore, discriminant validity is assessed by comparing the

square root of each construct's AVE with the inter-construct correlations. Constructs demonstrate adequate discriminant validity when the square root of their AVE values is higher than their correlations with other constructs, indicating that each construct is conceptually distinct and captures unique variance not explained by other variables in the model. This step ensures that AITI, TDA, RE, and CR measure different conceptual domains and do not overlap excessively, thus strengthening the overall validity of the structural model.

Table 2. Fornell–Larcker

Construct	AITI	TDA	RE	CR
AITI	0.888	0.691	0.673	0.642
TDA	0.691	0.895	0.709	0.725
RE	0.673	0.709	0.891	0.748
CR	0.642	0.725	0.748	0.898

Table 2 presents the Fornell–Larcker Criterion results, which demonstrate that discriminant validity is fully satisfied for all constructs in the measurement model. The diagonal values, representing the square roots of the AVE for each construct (AITI = 0.888, TDA = 0.895, RE = 0.891, CR = 0.898), are higher than their corresponding inter-construct correlations, confirming that each construct shares more variance with its own indicators than with those of other constructs. For instance, the square root of AVE for AI-Based Threat Intelligence (0.888) exceeds its correlations with TDA (0.691), RE (0.673), and CR (0.642), indicating clear conceptual distinctiveness. Similarly, Threat Detection Accuracy (0.895) shows stronger internal coherence compared to its correlations with RE (0.709) and CR (0.725). The same pattern is observed for Response Effectiveness and Cybersecurity Resilience, whose square root AVE values surpass all inter-construct correlations, demonstrating that the constructs are empirically distinguishable and do not exhibit multicollinearity issues. Overall, these results confirm that the measurement model possesses strong discriminant validity, ensuring that each latent construct captures unique conceptual dimensions within the structural framework.

Reliability analysis, assessed using Cronbach's Alpha and Composite Reliability with thresholds greater than 0.70, shows that all constructs in this study demonstrate excellent internal consistency. As presented in the table, AI-Based Threat Intelligence (AITI), Threat Detection Accuracy (TDA), Response Effectiveness (RE), and Cybersecurity Resilience (CR) achieve Cronbach's Alpha values ranging from 0.931 to 0.942 and Composite Reliability values from 0.949 to 0.956, all exceeding 0.90. These results indicate that the measurement items within each construct are highly consistent, stable, and reliable for capturing the underlying theoretical concepts, ensuring robustness in subsequent structural model analysis.

4.3 Structural Model Evaluation (Inner Model)

Structural model (inner model) evaluation was performed to assess the explanatory power (R^2), predictive relevance (Q^2), multicollinearity (VIF), path coefficients, and effect sizes (f^2) among the constructs using SEM-PLS 3 with 5,000 bootstrapping resamples. The R^2 results show that AI-Based Threat Intelligence (AITI) explains a moderate proportion of variance in both Threat Detection Accuracy (TDA) (R^2 = 0.477) and Response Effectiveness (RE) (R^2 = 0.453), indicating that AI-driven capabilities substantially enhance detection and response mechanisms.

Meanwhile, Cybersecurity Resilience (CR) shows a high explanatory power with $R^2 = 0.712$, demonstrating that AITI, TDA, and RE jointly explain 71.2% of the variance in organizational resilience. These findings confirm that the proposed model possesses strong predictive capability for its key outcome, cybersecurity resilience, and that improvements in AI-based intelligence, detection accuracy, and response effectiveness contribute meaningfully to strengthening resilience outcomes in cloud environments.

Predictive relevance of the model was further validated through the blindfolding procedure using cross-validated redundancy (Q^2). All endogenous constructs recorded Q^2 values greater than zero—TDA (0.332), RE (0.317), and CR (0.489)—indicating that the model has good predictive relevance, particularly for cybersecurity resilience, which shows the strongest predictive power. These results confirm that the structural model not only explains a substantial portion of variance but also accurately predicts unseen data patterns, reinforcing the robustness of the proposed framework. Additionally, assessment of Variance Inflation Factor (VIF) values ensures that multicollinearity is not present among predictor variables, further supporting the reliability of the structural relationships.

Table 3. VIF

Endogenous Construct	Predictor	VIF
Threat Detection Accuracy (TDA)	AI-Based Threat Intelligence (AITI)	1.000
Response Effectiveness (RE)	AI-Based Threat Intelligence (AITI)	1.000
Cybersecurity Resilience (CR)	AI-Based Threat Intelligence (AITI)	2.134
Cybersecurity Resilience (CR)	Threat Detection Accuracy (TDA)	2.768
Cybersecurity Resilience (CR)	Response Effectiveness (RE)	2.951

Table 3 presents the Variance Inflation Factor (VIF) values used to assess multicollinearity among predictor variables in the structural model, and the results indicate that all VIF values fall well below the conservative cutoff of 5.0, demonstrating that multicollinearity is not a concern in this study. For the constructs Threat Detection Accuracy (TDA) and Response Effectiveness (RE), the VIF value of 1.000 for AI-Based Threat Intelligence (AITI) shows that AITI is the sole predictor and exhibits no collinearity issues. For Cybersecurity Resilience (CR), the predictors AITI (VIF = 2.134), TDA (VIF = 2.768), and RE (VIF = 2.951) all remain within acceptable thresholds, indicating that although the predictors are conceptually related, they do not exhibit problematic overlap or redundancy in explaining CR. This confirms that each predictor contributes unique explanatory power to the model, and that the relationships among AITI, TDA, RE, and CR can be interpreted with confidence without concerns of inflated standard errors or unstable path estimates. Overall, the VIF results reinforce the robustness and statistical reliability of the structural model.

4.4 Path Coefficients and Hypothesis Testing

Path coefficients (β), t-statistics, and p-values were obtained through bootstrapping (5,000 resamples) to test the significance and direction of the hypothesized relationships.

Table 4. Path Coefficients and Hypothesis Testing

Path	Coefficient (β)	t-Statistic	p-Value	Result
H1: AITI → TDA	0.691	13.457	< 0.001	Supported
H2: AITI → RE	0.673	12.038	< 0.001	Supported
H3: TDA → CR	0.311	4.892	< 0.001	Supported
H4: RE → CR	0.428	7.125	< 0.001	Supported

Path	Coefficient (β)	t-Statistic	p-Value	Result
H5: AITI → CR	0.204	3.021	0.003	Supported

Table 4 presents the results of the path coefficient analysis and hypothesis testing, showing that all proposed hypotheses (H1–H5) are statistically supported. The strong and highly significant relationship between AI-Based Threat Intelligence (AITI) and both Threat Detection Accuracy (TDA) ($\beta = 0.691$, $t = 13.457$, $p < 0.001$) and Response Effectiveness (RE) ($\beta = 0.673$, $t = 12.038$, $p < 0.001$) confirms that AI-driven intelligence substantially enhances core operational mechanisms within cybersecurity systems. Furthermore, both TDA ($\beta = 0.311$, $t = 4.892$, $p < 0.001$) and RE ($\beta = 0.428$, $t = 7.125$, $p < 0.001$) demonstrate significant positive effects on Cybersecurity Resilience (CR), indicating that accurate threat detection and effective response execution are critical pathways through which resilience is strengthened. Although smaller in magnitude compared to the mediating pathways, the direct effect of AITI on CR ($\beta = 0.204$, $t = 3.021$, $p = 0.003$) remains statistically significant, suggesting that AI-based threat intelligence not only influences resilience indirectly but also contributes to resilience improvements at a strategic level. Collectively, these results validate the conceptual model and empirically demonstrate that AITI enhances cybersecurity resilience both directly and through the mechanisms of improved detection accuracy and response effectiveness.

Effect size (f^2) was used to assess the relative contribution of each exogenous construct on its endogenous construct. Values of $f^2 \approx 0.02$, 0.15, and 0.35 are interpreted as small, medium, and large effects, respectively.

Table 5. Effect Size (f^2) of Exogenous Variables

Endogenous Construct	Predictor	f^2	Effect Size Interpretation
Threat Detection Accuracy (TDA)	AI-Based Threat Intelligence (AITI)	0.911	Large
Response Effectiveness (RE)	AI-Based Threat Intelligence (AITI)	0.833	Large
Cybersecurity Resilience (CR)	AI-Based Threat Intelligence (AITI)	0.075	Small
Cybersecurity Resilience (CR)	Threat Detection Accuracy (TDA)	0.196	Medium
Cybersecurity Resilience (CR)	Response Effectiveness (RE)	0.292	Medium–Large

Table 5 provides the effect size (f^2) results, which illustrate the magnitude of influence each exogenous variable exerts on its respective endogenous construct. AI-Based Threat Intelligence (AITI) demonstrates a large effect on both Threat Detection Accuracy (TDA) ($f^2 = 0.911$) and Response Effectiveness (RE) ($f^2 = 0.833$), indicating that enhancements in AI-driven threat intelligence substantially improve an organization's ability to detect and respond to cyber threats—consistent with the model's theoretical assumptions. In contrast, AITI shows only a small direct effect on Cybersecurity Resilience (CR) ($f^2 = 0.075$), suggesting that AI contributes to resilience more significantly through indirect pathways rather than as a standalone factor. These indirect pathways are evident in the medium effect of TDA on CR ($f^2 = 0.196$) and the medium-to-large effect of RE on CR ($f^2 = 0.292$), which confirms that improvements in detection accuracy and response effectiveness play a crucial mediating role in strengthening cybersecurity resilience. Overall, the effect size results reinforce the structural model's logic: AI-based threat intelligence has its greatest impact on operational cybersecurity functions (detection and response), which in turn are the primary drivers of organizational resilience in cloud environments.

4.5 Discussion

The results confirm that AI-Based Threat Intelligence has a strong and significant positive effect on Threat Detection Accuracy, demonstrating that organizations adopting AI-driven security mechanisms are substantially more capable of identifying cyber threats accurately, including unknown and zero-day attacks. This reinforces the shift from traditional signature-based systems toward behavioral and learning-based detection models, which are far more suited to cloud environments characterized by massive, dynamic, and distributed data flows that conventional tools often fail to analyze effectively. In Indonesia, where cybersecurity maturity varies widely across organizations, the strong influence of AI on detection accuracy indicates a critical opportunity for compensating shortages in specialized cybersecurity talent and improving national cybersecurity capacity in cloud-based ecosystems.

The findings also show that AI-Based Threat Intelligence significantly enhances Response Effectiveness, enabling faster, more accurate, and more coordinated cyber incident handling through automated containment, real-time threat blocking, and intelligent orchestration processes. This supports the principle that modern cyber response must operate at machine speed, particularly in cloud infrastructures where attacks can propagate across virtualized resources within seconds. For Indonesian organizations increasingly dependent on cloud platforms for public services, financial transactions, and digital operations, this improvement in response capability directly contributes to operational continuity and strengthens organizational readiness in the face of escalating cyber threats [32], [33].

Additionally, the analysis reveals that Threat Detection Accuracy and Response Effectiveness each exert a significant positive effect on Cybersecurity Resilience. Accurate and early detection enables organizations to prevent large-scale service disruptions and limit the impact of cyber incidents, aligning with resilience theory that emphasizes anticipation and early warning as foundational components of resilient systems [34], [35]. In Indonesia's cloud ecosystem—where redundancy, preparedness, and incident response maturity may vary—enhanced detection and response capabilities serve not only as protective measures but also as strategic investments for long-term resilience in digital infrastructures.

Finally, the study confirms that AI-Based Threat Intelligence also has a direct and significant effect on Cybersecurity Resilience, indicating that AI contributes not only through improved detection and response mechanisms but also through broader organizational capabilities such as predictive awareness, adaptive learning, and continuous improvement. Mediation analysis further shows that Threat Detection Accuracy and Response Effectiveness partially mediate the relationship between AI-Based Threat Intelligence and Cybersecurity Resilience, confirming a closed-loop cybersecurity model in which AI enhances detection, improved detection strengthens response, and effective response reinforces overall resilience. This dynamic interaction mirrors adaptive cybersecurity principles and demonstrates that AI should be positioned as a strategic driver of resilience development within Indonesia's rapidly expanding digital landscape.

4.6 Implications for Indonesian Cloud Infrastructure Security

The discussion of findings carries important implications for Indonesia's digital transformation and national cybersecurity strategy, particularly as cloud adoption expands across government, financial institutions, education, healthcare, and SMEs, rendering conventional security systems increasingly inadequate. This study

provides empirical evidence that AI-based threat intelligence is fundamental for achieving sustainable cybersecurity resilience in cloud environments. For policymakers, the results underscore the need to strengthen regulatory frameworks, create incentives for AI adoption, and invest in workforce development in AI and digital security. For cloud service providers, the findings highlight the importance of embedding AI-driven security mechanisms as core infrastructure components rather than optional features. For organizations, the study demonstrates that the highest level of cybersecurity resilience is achieved through integrated systems that combine accurate threat detection, rapid and effective response, and continuous adaptive intelligence.

4.7 Theoretical Contributions

From a theoretical perspective, this study contributes to the cybersecurity and information systems literature by empirically validating an AI-driven cybersecurity resilience model using SEM-PLS and by integrating threat detection accuracy and response effectiveness as mediating variables, thereby expanding the understanding of how AI operationalizes resilience in cloud environments. The findings also strengthen resilience theory by positioning AI-based threat intelligence as a dynamic and strategic organizational capability rather than merely a technical tool, while the contextualization of the model within the Indonesian cloud ecosystem enriches the literature on cybersecurity resilience in emerging digital economies.

5. CONCLUSION

This study provides strong empirical evidence that Artificial Intelligence-based threat intelligence plays a critical role in strengthening cybersecurity resilience in Indonesian cloud infrastructure. The results confirm that AI-based threat intelligence significantly improves threat detection accuracy and response effectiveness, which in turn enhance organizational cybersecurity resilience, while also exerting a direct influence through strengthened predictive awareness, adaptive learning, and continuous security improvement. The findings emphasize that cybersecurity resilience is not solely determined by preventive controls, but also by the organization's ability to accurately detect threats and respond swiftly to cyber incidents; in highly interconnected cloud environments, delays in these processes can trigger cascading failures, making AI-driven intelligence essential for ensuring service continuity, protecting critical assets, and maintaining public trust.

From a strategic standpoint, the study confirms that AI-based cybersecurity is not merely a technological enhancement but a core organizational capability that enables a shift from reactive to proactive and adaptive defense strategies, positioning AI adoption as a long-term resilience-building investment for Indonesian organizations increasingly reliant on cloud infrastructure. The study also offers theoretical contributions by validating an AI-driven resilience model that integrates detection accuracy and response effectiveness as mediating mechanisms, while situating the model within the Indonesian digital ecosystem to expand empirical understanding of cybersecurity resilience in emerging economies; however, limitations such as its cross-sectional design and perception-based data suggest the need for future research using longitudinal methods, experimental simulations, and technical performance metrics, as well as exploring AI integration with blockchain, zero-trust architectures, and national cyber defense frameworks.

REFERENCE

[1] R. A. Sunarjo *et al.*, "Addressing Cybersecurity Risks in Multi Cloud Environments for Digital Transformation," in *2025 4th International Conference on Creative Communication and Innovative Technology (ICCIT)*, 2025, pp. 1–6.

[2] G. Lambropoulos, S. Mitropoulos, and C. Douligeris, "A Review on Cloud Computing services, concerns, and security risk awareness in the context of Digital Transformation," in *2021 6th South-East Europe Design Automation,*

Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2021, pp. 1–6.

[3] M. E. Abimanyu, S. Ratnaningtyas, and S. Hutajulu, "Cloud Computing Adoption Strategy for Government Sector in Indonesian Cloud Industry," *Int. J. Bus. Technol. Manag.*, vol. 6, no. 2, pp. 438–444, 2024.

[4] M. Natti, "Cloud and on-premise DBaaS (Database as a Service) - PostgreSQL Database Deployments automation," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 9, no. 2, pp. 772–776, 2023.

[5] T. Haryanti, N. A. Rakhmawati, and A. P. Subriadi, "Navigating the Digital Transformation Landscape in Indonesia: A Qualitative Sectoral Analysis," in *2024 IEEE International Symposium on Consumer Technology (ISCT)*, 2024, pp. 805–811.

[6] J. M. DWI, K. W. IDK, S. ADI, W. PUJO, and K. KUSUMA, "Digital World Threat Preparedness For Digital Transformation Acceleration Policy In Indonesia," *Int. J.*, vol. 4, no. 1, 2024.

[7] V. Jyothsna, E. Sandhya, K. B. Kamalapuram, and P. Bhasha, "AI-Driven Threat Detection in Cloud Environments," in *Convergence of Cybersecurity and Cloud Computing*, IGI Global Scientific Publishing, 2025, pp. 261–284.

[8] C. Harshvardhan And C. Pratikkumar, "Enhancing cybersecurity in cloud environments using AI-driven threat detection and response," *Int. J.*, vol. 3, no. 1, pp. 13–30, 2024.

[9] D. Chaudhary, S. K. Verma, V. M. Shrimal, R. Madala, and R. Baliyan, "Ai-based methods to detect and counter cyber threats in cloud environments to strengthen cloud security," in *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, 2024, vol. 1, pp. 1–6.

[10] A. B. Dorothy, B. Madhavidevi, B. Nachiappan, G. Manikandan, P. K. Patjoshi, and M. Sindhuja, "AI-Driven Threat Intelligence in Cloud Computing Detecting and Responding to Cyber Attacks," in *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, 2024, pp. 1–6.

[11] P. Chuwattanakul, *Perceived leadership style, style flexibility, and style effectiveness of government hospital administrators in Thailand*. Andrews University, 1993.

[12] X. Sun, P. Liu, and A. Singhal, "Toward cyberresiliency in the context of cloud computing [resilient security]," *IEEE Secur. Priv.*, vol. 16, no. 6, pp. 71–75, 2018.

[13] K. AGUS, "Study of the Artificial Intelligence Role in Achieving Cybersecurity for Critical Information Infrastructure," *MONAS J. Inov. Apar. Учредители Badan Pengemb. Sumber Daya Mns. Provinsi DKI Jakarta*, vol. 6, no. 2, pp. 154–165, 2024.

[14] K. Saraswati, B. Purwandari, and N. W. Trisnawaty, "Investigating Challenges in Information Security Governance Implementation in Key Sectors: A Cross-Country Comparative Analysis," *Indones. J. Comput. Sci.*, vol. 14, no. 2, 2025.

[15] R. Kurniawan, A. Subroto, and E. Daryanto, "A Systematic Literature Review of Organizational Resilience In Indonesia," *Asian J. Eng. Soc. Heal.*, vol. 3, no. 4, pp. 893–902, 2024.

[16] M. J. Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," *Masy. Telemat. Dan Inf. J. Penelit. Teknol. Inf. Dan Komun.*, vol. 8, no. 2, pp. 137–144, 2018.

[17] S. S. Aulianisa and I. Indirwan, "Critical review of the urgency of strengthening the implementation of cyber security and resilience in Indonesia," *Lex Sci. Law Rev.*, vol. 4, no. 1, pp. 31–45, 2020.

[18] M. Akinsanya, "Next-Generation Cyber Resilience Frameworks: Enhancing Security, Recovery, And Continuity In Modern Networked Systems," *Int. J. Sci. Technol.*, vol. 3, no. 1, pp. 1–14, 2024.

[19] N. Parvatha, "Resilient cybersecurity frameworks for multi-cloud environment: Innovations in securing distributed systems against emerging threats," *Int. J. Sci. Res. Arch.*, vol. 3, no. 1, pp. 266–275, 2021.

[20] R. C. Srinivas, "Ai-Driven Security Posture Management: A Revolutionary Approach To Multi-Cloud Enterprise Security," *Int. J.*, vol. 11, no. 1, pp. 497–509, 2025.

[21] A. Singhal, P. Liu, and X. Sun, "Towards Cyber Resiliency in the Context of Cloud Computing".

[22] V. Kiranmai and A. Manikandan, "Global Journal of Engineering Innovations & Interdisciplinary Research Original Article A Study on AI-Powered Threat Intelligence Systems for Proactive Cyber Defence," vol. 5, no. 5, pp. 1–4, 2025.

[23] C. Ucheji, J. Ekeneme, and C. Ezekwem, "Global Trends in AI-Driven Cybersecurity: A Systematic and Bibliometric Analysis," *Asian J. Res. Comput. Sci.*, vol. 18, no. 9, pp. 103–115, 2025.

[24] M. M. Rahman, K. Dhakal, N. Gony, M. K. Shuvra, and M. Rahman, "AI integration in cybersecurity software: Threat detection and response," *Int. J. Innov. Res. Sci. Stud. [Internet]*, pp. 3907–3921, 2025.

[25] R. Sissodia, M. S. Rauthan, V. Barthwal, and V. Dwivedi, "Artificial Intelligence (AI) in Cybersecurity," *Adv. Cybersecurity Smart Factories Through Auton. Robot. Defenses*, pp. 121–152, 2025.

[26] S. Thapaliya, "Artificial Intelligence and Cybersecurity: Pioneering Next-Generation Protection Strategies," *SADGAMAYA*, vol. 2, no. 1, pp. 61–65, 2025.

[27] M. Sameer and F. M. Khan, "AI Threat Detection," 2025.

[28] S. Oduri, "AI-Powered threat detection in cloud environments," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 9, no. 12, pp. 57–62, 2021.

[29] D. G. Patel and S. R. Pujari, "AI-driven incident response in cloud security," 2025.

[30] M. A. M. Farzaan, M. C. Ghanem, A. El-Hajjar, and D. N. Ratnayake, "Ai-enabled system for efficient and effective cyber incident detection and response in cloud environments," *arXiv Prepr. arXiv2404.05602*, 2024.

[31] S. Tatineni, "AI-infused threat detection and incident response in cloud security," *Int. J. Sci. Res.*, vol. 12, no. 11, pp. 998–1004, 2023.

[32] S. Sood and A. Kim, "The Golden Age of the Big Data Audit: Agile Practices and Innovations for E-Commerce, Post-Quantum Cryptography, Psychosocial Hazards, Artificial Intelligence Algorithm Audits, and Deepfakes," *Int. J. Innov. Econ. Dev.*, vol. 9, no. 2, pp. 7–23, 2023, doi: 10.18775/ijied.1849-7551-7020.2015.92.2001.

[33] P. J. Nesse, H. S. Hallingby, and ..., "Validation of 5G use case solutions–Simultaneous assessment of business value

and social acceptance in early stages of the research and innovation …," … *and Technology*. journal.riverpublishers.com, 2023.

[34] O. A. Farayola, "Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity," *Financ. Account. Res. J.*, vol. 6, no. 4, pp. 501–514, 2024.

[35] A. K. Ahmed and A. A. Khorsheed, "Open network structure and smart network to sharing cybersecurity within the 5G network," *Indonesian Journal of Electrical* …. researchgate.net, 2022.