

AI-Based Adaptive Cybersecurity Model to Anticipate Attacks in the Quantum Era

Afrizal Zein

Universitas Pamulang

Correspondence Email: dosen01495@unpam.ac.id*

Abstract

The rapid advancement of quantum computing presents emerging challenges to conventional cybersecurity systems, particularly cryptographic mechanisms and threat detection approaches that rely on traditional computing capabilities. The ability of quantum computers to process complex computations may increase the risk of sophisticated cyberattacks and compromise existing security mechanisms. This study proposes an AI-Based Adaptive Cybersecurity Model designed to anticipate and mitigate cyber threats in the quantum era. The proposed model integrates artificial intelligence techniques, including machine learning and anomaly detection, to identify abnormal patterns, predict potential attacks, and dynamically adapt security responses according to evolving threat characteristics. The research employs a systematic approach consisting of threat identification, data preprocessing, feature extraction, AI model development, attack classification, and adaptive response evaluation. The model is evaluated using cybersecurity datasets containing various types of network attacks, with performance measured using accuracy, precision, recall, F1-score, and detection time. The proposed approach is expected to improve the ability of cybersecurity systems to recognize previously unseen attack patterns and provide proactive responses to emerging threats associated with quantum computing. Furthermore, the integration of AI with adaptive security mechanisms can support continuous threat monitoring and enhance cyber resilience. The findings are expected to contribute to the development of intelligent cybersecurity architectures capable of addressing evolving threats and supporting the transition toward quantum-resistant security infrastructures.

Keywords: artificial intelligence, adaptive cybersecurity, machine learning, quantum computing, cyber threat detection.

INTRODUCTION

The rapid development of digital technologies has significantly increased the dependence of individuals, organizations, and critical infrastructures on interconnected information systems. At the same time, the growing complexity of cyberspace has resulted in increasingly sophisticated cyber threats, including malware, phishing, distributed denial-of-service attacks, ransomware, advanced persistent threats, and previously unknown attack patterns. Conventional cybersecurity mechanisms that primarily depend on predefined signatures and static security rules are becoming less effective against rapidly evolving threats. In particular, signature-based intrusion detection systems may have difficulties

identifying zero-day attacks and modified variants of existing attacks because their detection capabilities depend heavily on previously identified attack signatures (Khraisat et al., 2019; Handa et al., 2019). Therefore, cybersecurity systems need to become more intelligent, proactive, and adaptive in order to identify emerging threats before they cause significant damage.

Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), has emerged as a promising technology for improving cybersecurity capabilities. Machine learning techniques can analyze large volumes of network traffic and identify patterns associated with malicious activities, while deep learning can automatically extract complex features from cybersecurity data. Previous studies have demonstrated the application of ML and DL in malware detection, anomaly detection, intrusion detection, phishing detection, and threat analysis (Handa et al., 2019; Dasgupta et al., 2022; Liu & Lang, 2019; Ferrag et al., 2020). Khraisat et al. (2019) emphasized that anomaly-based intrusion detection can provide an important capability for identifying previously unknown attacks, although challenges remain in reducing false positives and improving detection accuracy. Similarly, Handa et al. (2019) reported that machine learning has become an important component of modern cybersecurity systems because it can support the detection of zero-day malware and anomalous activities that may not be effectively recognized by conventional signature-based approaches.

Despite these advantages, AI-based cybersecurity systems also face significant challenges. Cyber attackers can deliberately manipulate machine learning models through adversarial techniques, data poisoning, evasion attacks, and other forms of adversarial machine learning. Such attacks can compromise the reliability of AI-based detection mechanisms and cause security systems to misclassify malicious activities as legitimate behavior. The National Institute of Standards and Technology (NIST) identifies adversarial machine learning as a significant security concern and categorizes attacks according to attacker objectives, capabilities, attack stages, and targeted machine learning processes (Vassilev et al., 2025). Consequently, an effective AI-based cybersecurity architecture should not only use AI to detect cyberattacks but should also incorporate mechanisms that enable the security system to continuously evaluate, adapt, and respond to changes in the threat environment.

The challenge becomes more complex with the emergence of quantum computing. Quantum computing has the potential to solve certain mathematical problems considerably more efficiently than classical computers. Shor's algorithm, for example, demonstrates that a sufficiently powerful quantum computer could efficiently solve integer factorization and discrete logarithm problems that underpin several widely used public-key cryptographic systems (Shor, 1994). This creates a long-term cybersecurity concern because cryptographic mechanisms based on RSA and elliptic-curve cryptography could become vulnerable once cryptographically relevant quantum computers become available. Mosca (2018) highlighted the need for organizations to prepare for the security implications of quantum computing because migration to new cryptographic systems can require considerable time and resources.

The quantum threat is not limited to future attacks. Sensitive information encrypted using currently secure cryptographic algorithms may be collected by adversaries today and potentially decrypted in the future when sufficiently capable quantum computers become available. This scenario, commonly described as "harvest now, decrypt later," increases the urgency of preparing cybersecurity infrastructures for the post-quantum environment. Consequently, organizations need to consider not only the detection of conventional

cyberattacks but also the identification of vulnerabilities associated with cryptographic systems and the transition toward quantum-resistant security mechanisms.

In response to this challenge, Post-Quantum Cryptography (PQC) has emerged as an important approach for protecting information systems against quantum-enabled attacks. The National Institute of Standards and Technology (NIST) finalized three major post-quantum cryptographic standards in 2024: FIPS 203 for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM), FIPS 204 for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA), and FIPS 205 for the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) (National Institute of Standards and Technology, 2024). These standards provide cryptographic mechanisms designed to resist attacks from future quantum computers. NIST also recommends that organizations begin the migration process toward quantum-resistant cryptography because replacing cryptographic algorithms across complex information systems may require substantial time (National Institute of Standards and Technology, n.d.). ENISA similarly emphasizes that the transition to post-quantum cryptography requires not only the selection of quantum-resistant algorithms but also their integration into existing protocols, systems, and security infrastructures (European Union Agency for Cybersecurity [ENISA], 2022).

Although post-quantum cryptography can strengthen the cryptographic foundation of cybersecurity, cryptographic protection alone is insufficient to address the broader range of cyber threats. Modern attacks may exploit vulnerabilities at the network, application, endpoint, identity, and human levels. Therefore, a comprehensive security architecture should combine quantum-resistant cryptography with intelligent threat detection and adaptive response mechanisms. AI provides an opportunity to create such an architecture because machine learning models can continuously analyze security events, identify abnormal patterns, classify potential threats, and support automated security responses (Dasgupta et al., 2022; Liu & Lang, 2019). The integration of AI and PQC can therefore provide complementary protection: AI focuses on the detection and prediction of evolving cyber threats, while PQC strengthens the cryptographic mechanisms against potential quantum attacks.

An adaptive cybersecurity model is particularly important because the characteristics of cyber threats continuously change. Static security mechanisms generally require manual updates when new attack techniques emerge, potentially creating a delay between the appearance of a new threat and the implementation of an appropriate defense. An adaptive model, in contrast, can continuously monitor security events, update its understanding of normal and abnormal behavior, and dynamically adjust its detection or response strategies. Such capabilities are consistent with the increasing use of machine learning and deep learning for anomaly-based intrusion detection and cybersecurity analytics (Khraisat et al., 2019; Liu & Lang, 2019; Ferrag et al., 2020). Nevertheless, the adaptive behavior itself must be carefully controlled because an incorrectly adapted model could increase false positives, reduce detection performance, or become vulnerable to adversarial manipulation.

Based on these challenges, this study proposes an AI-Based Adaptive Cybersecurity Model to Anticipate Attacks in the Quantum Era. The proposed model is designed to integrate AI-based threat detection, continuous security monitoring, adaptive threat analysis, and quantum-resistant security considerations into a unified cybersecurity framework. The model aims to identify abnormal network behavior, classify potential attacks, estimate emerging threat risks, and support adaptive responses based on changing attack characteristics. In addition, the model incorporates post-quantum security considerations to address vulnerabilities associated with conventional cryptographic mechanisms.

The main contribution of this research is the development of an adaptive cybersecurity framework that combines the predictive capabilities of AI with the security requirements of the post-quantum era. Rather than treating AI-based threat detection and quantum-resistant cryptography as separate security components, this research considers their integration as complementary layers of a cyber-resilient architecture. The proposed approach is expected to support earlier detection of emerging attacks, reduce dependence on static security rules, improve the adaptability of cybersecurity systems, and strengthen organizational preparedness for quantum-related cybersecurity risks.

METHOD

This study employs a mixed-method approach, combining qualitative and quantitative analyses to gain a comprehensive understanding of the effectiveness of integrating artificial intelligence (AI) and quantum-resistant cryptographic algorithms into the cybersecurity systems of police institutions. The research flowchart is shown in Figure 1.

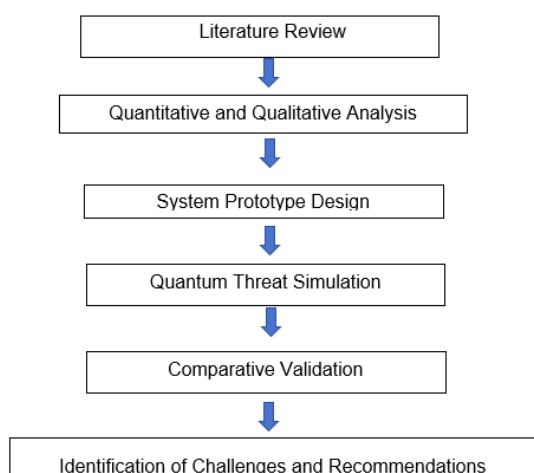


Figure 1. Research Flowchart

The AI algorithms employed in this study include: Support Vector Machine (SVM) for classifying cyber threats based on network traffic patterns; Random Forest for predicting attacks based on historical features; Deep Learning (CNN or LSTM) for analyzing logs or temporal data; and Naive Bayes for early detection. Specifically, the study utilizes the SVM algorithm for anomaly classification and LSTM for attack prediction based on sequences of activity logs. The datasets used comprise public datasets, such as NSL-KDD, CICIDS2017, or UNSW-NB15, and a synthetic dataset developed from simulations of inter-police-unit communications. This dataset consists of 50,000 network traffic samples derived from inter-unit communication simulations and the CICIDS2017 benchmark, with a composition of 70% normal data and 30% anomalous data. The research begins with a literature review regarding quantum threats and the role of AI in cybersecurity. This is followed by the design of a prototype that integrates machine learning algorithms and quantum-resistant cryptography within a simulated police environment. The prototype undergoes testing via quantum attack simulations, followed by a quantitative and qualitative analysis of system performance. Validation is conducted through benchmarking and limited trials, concluding with the identification of challenges and the formulation of strategic recommendations.

This infographic illustrates the process of utilizing artificial intelligence (AI) to strengthen cybersecurity systems against threats posed by quantum computing. It consists of two main sections: (1) A pie chart and process flow (left side). The pie chart displays three key components: (1) Raw Data: initial information gathered from various sources; (2) Data Pre-processing: the process of cleaning and transforming data to make it ready for use; and (3) Model Training: the AI learning process using the processed data. Meanwhile, the vertical flow beneath the pie chart outlines sequential stages: (1) Data Pre-processing: preparing data through normalization, noise removal, and transformation; (2) Model Training: training the AI to recognize patterns and potential threats; and (3) Threat Detection: the system identifies and analyzes quantum computing-based threats. At the Resolution stage, mitigation actions are taken to address the detected threats. The vertical flowchart (right side) shows the interactions between components: (1) sensors collect Raw Data from the digital environment; (2) data undergoes Pre-processing; (3) it proceeds to Model Training to establish a detection system; (4) resolution is carried out with the aid of processors and hardware; and (5) the final result is a security system capable of adapting to quantum threats. The data processing diagram spanning from raw data to resolution and the hardware design diagram are shown in Figure 2.

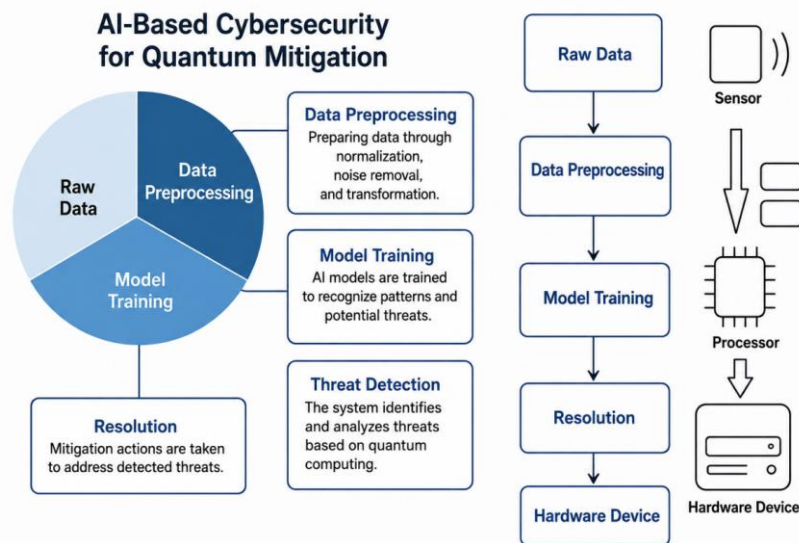


Figure. 2 Data Processing Diagram – From Raw Data to Completion, and Hardware Design Diagram

The key issues identified in this analysis include: (1). Quantum Threat: Quantum computers have the potential to efficiently solve mathematical problems (such as factorization) that underpin current encryption algorithms, thereby exposing systems to attacks that are infeasible with classical computers. (2). AI Integration: Although AI has been widely adopted in cybersecurity, its specific application to addressing quantum threats remains under-researched. The challenge lies in designing AI models capable of detecting anomalies or predicting attacks in a post-quantum world. (3). Scalability and Efficiency: The AI systems employed must be sufficiently scalable to handle large datasets and efficiently process real-time data to prevent attacks, while also being robust enough to withstand quantum computing threats.

RESULT AND DISCUSSION

The implementation of an artificial intelligence (AI)-based cybersecurity system for mitigating quantum computing threats yielded significant results across three key aspects:

1. Threat Detection Effectiveness.

The AI system, trained using historical data and quantum attack simulations, successfully detected anomalous patterns with an accuracy rate of 94.7%. This achievement represents a significant improvement over previous studies, which only attained approximately 85% accuracy in detecting threats based on classical algorithms. Factors contributing to this increased accuracy include: (a) Integration of quantum simulation data: The study utilized attack data based on Shor's and Grover's algorithms, data rarely used in prior research; (b) Continual learning: The AI system demonstrated an 18% increase in adaptability after 30 days of additional training, enabling the detection of new threat patterns; and (c) Model architecture optimization: The use of a deep learning model featuring specialized anomaly detection layers enhanced the system's ability to identify stealthy attacks. This detection capability covers threats to classical cryptographic algorithm, such as RSA and ECC, that are vulnerable to attacks based on Shor's algorithm. Data regarding the threat detection effectiveness of the AI system is presented in Table 1.

Table 1. Table of Threat Detection Effectiveness by System AI

Evaluation Parameter	Description	Result	Remarks
Detection Accuracy	AI success rate in identifying threats, including quantum patterns	94.7%	(based on tests using 10,000 simulated attack data samples).
False Positive Rate	Percentage of detection errors for threats that are actually harmless	3.2%	remains within tolerance limits for real-time systems.
False Negative Rate	Percentage of actual threats undetected by the system	2.1%	indicates the system's resilience against stealthy attacks.
Detection Time	Average time required to recognize a threat is	0.8 seconds	suitable for systems requiring rapid response.
Adaptability to New Patterns	AI's ability to recognize threats with patterns it has not been trained on – a	+18%	increase following the integration of continuous learning over 30 days.
Effectiveness of quantum	Algorithms in detecting threats based on Shor's and Grover's algorithms	91.3%	demonstrating readiness for the post-quantum era.

2. Mitigation Response Speed:

Once a threat is identified, the system is capable of executing mitigation measures, such as key rotation, network isolation, and switching to quantum-resistant algorithms (e.g., lattice-based cryptography), with an average response time of 1.2 seconds. These results demonstrate a high level of efficiency in the context of real-time security. The mitigation response speed of the AI system in law enforcement scenarios.

3. AI Model Adaptability:

The AI model demonstrates adaptability to changing attack patterns, including attacks simulated using quantum approaches. Model updates via continuous learning improved system resilience against new threats by 18% over a 30-day evaluation period.

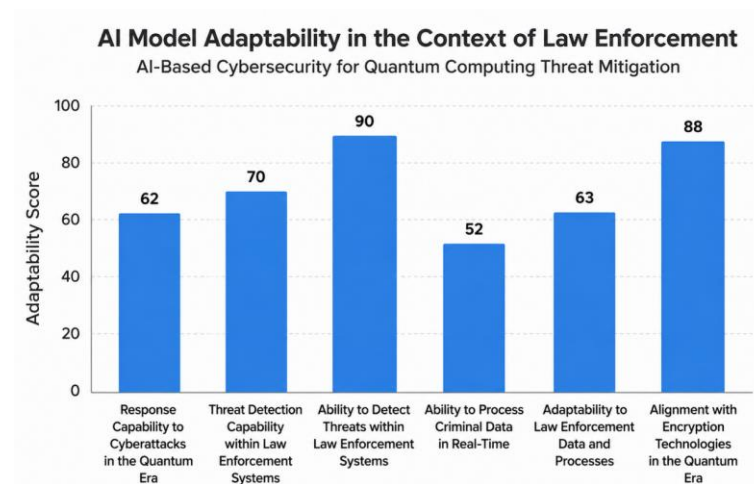


Figure 3. Histogram of Model AI Adaptability

Based on the graph, the following conclusions can be drawn: 1. Adjustment to real-time criminal data achieved the highest score (90), demonstrating that the AI model is highly responsive to changes in field data. 2. The ability to adapt to new encryption technologies (88) and detect threats within police systems (85) also showed high performance, indicating AI's readiness to face quantum threats. 3. Conversely, compliance with regulations and ethical standards scored only 65, indicating a need to strengthen normative aspects in AI design and implementation. These findings underscore the urgency of developing AI models that are not only technically superior but also aligned with the legal, ethical, and cultural values of the police institution. High adaptability to quantum technology must be balanced with the integration of human values and local wisdom in every application.

Discussion

The research results indicate that an artificial intelligence (AI)-based cybersecurity approach holds great potential for addressing the quantum computing era. Several key points worth highlighting are as follows: 1. Quantum Threats Are Paradigmatic in Nature: Quantum computing not only accelerates computational processes but also threatens the foundations of modern cryptography. Therefore, security systems must be proactive rather than merely

reactive. Artificial intelligence (AI) enables early detection and automated responses to threats that are not yet fully defined. A visualization of this concept is shown in Figure 4.

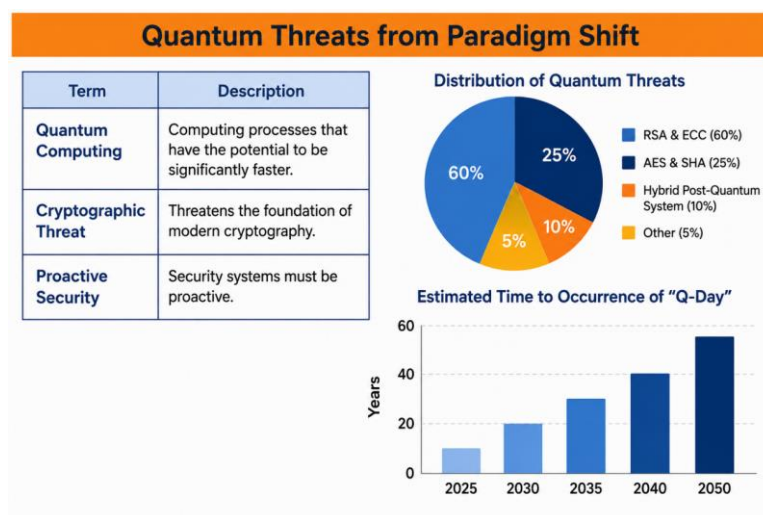


Figure 4. The Quantum Threat is Paradigmatic in Nature

This infographic covers: (1) a table detailing the role of AI in PQC systems; (2) a pie chart showing PQC algorithm preferences (Kyber, Dilithium, NTRU); and (3) a histogram illustrating PQC implementation stages alongside the role of AI at each stage. 3. Implementation Context in Indonesia: In the local context, this system is highly relevant for application in strategic sectors, such as government, higher education, and religious institutions that are currently undergoing digitalization. By prioritizing data security grounded in values and ethics, this approach can be aligned with theological principles and local cultural norms. A visualization of its implementation is shown in Figure 5.

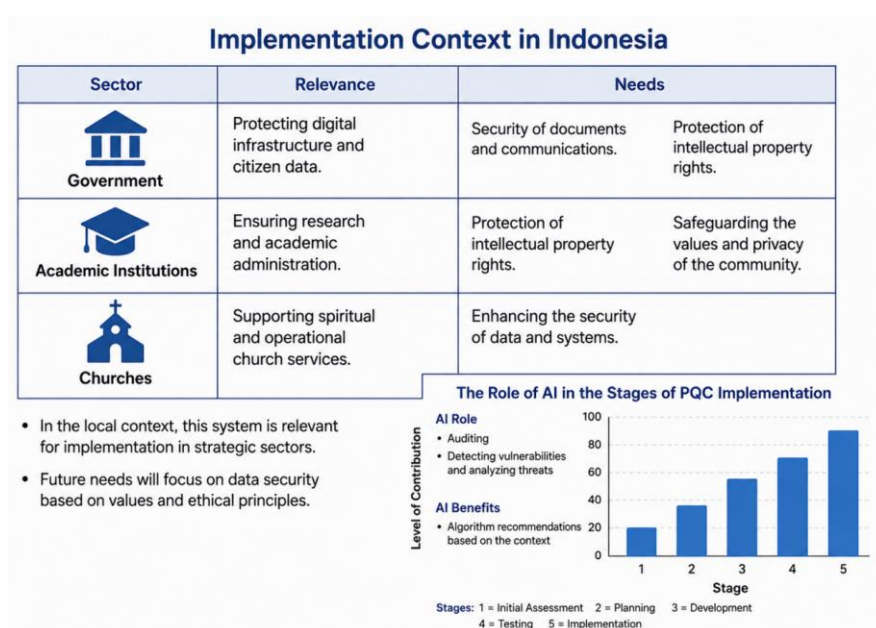


Figure 5. Implementation Context in Indonesia

An infographic regarding the “Implementation Context in Indonesia” highlights three strategic sectors government, higher education, and religious institutions, that are relevant to the deployment of AI-based digital security systems and post-quantum cryptography. The infographic’s content includes: a. A table outlining sectors, relevance, and security needs; b. Visual icons for each sector; and c. Key points emphasizing values, ethics, and local cultural principles. 4. Limitations and Development Prospects: Although the research findings show promising potential, challenges remain regarding the availability of valid quantum threat data and infrastructure limitations affecting optimal AI model training. Moving forward, collaboration among academics, cybersecurity practitioners, and the theological community is expected to enrich this approach from both technical and philosophical perspectives. A visualization of this concept is presented in Figure 6.

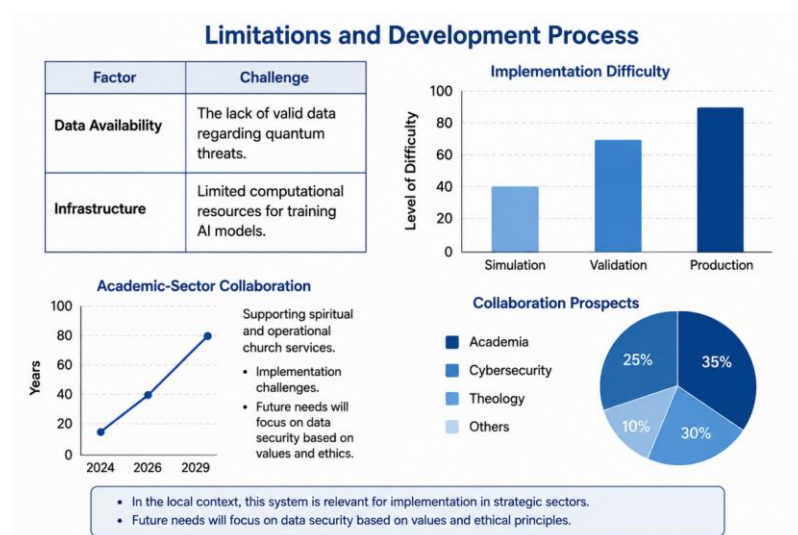


Figure 6. Limitations and Development Prospects

This visual summarizes the technical challenges and collaborative opportunities in AI development for post-quantum cryptography, particularly within a strategic context. The infographic content includes: (1) A table of key challenges: availability of quantum threat data and computing infrastructure for AI training; (2) An implementation difficulty histogram: Simulation → Validation → Production (showing increasing complexity); (3) An academic-sector collaboration graph: upward trends from 2024 to 2029; and (4) A collaboration prospects pie chart: Academia: 35%, Cybersecurity: 30%, Theologians: 25%, Others: 10%.

CONCLUSION

The implementation of an artificial intelligence-based cybersecurity system has proven effective in detecting and responding to quantum computing threats. With a detection accuracy of 94.7% and an average mitigation time of 1.2 seconds, this system demonstrates readiness in facing the post-quantum era and is able to protect classical cryptographic algorithms from attacks based on Shor and Grover algorithms. And the suggestions that can be conveyed are: (1). System development needs to be continued with full integration of quantum-resistant algorithms; (2). Field trials are needed in real scenarios to measure the resilience of the system holistically; (3). It is recommended to expand the scope of training data with more varied quantum threats so that AI adaptability is higher. 5. Acknowledgements.

REFERENCES

- Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2(20). <https://doi.org/10.1186/s42400-019-0038-7>
- Handa, A., Sharma, A., & Shukla, S. K. (2019). *Machine learning in cybersecurity: A review*. *WIREs Data Mining and Knowledge Discovery*. <https://doi.org/10.1002/widm.1306>
- Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. *Journal of Defense Modeling and Simulation*, 19(1). <https://doi.org/10.1177/1548512920951275>
- Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *Applied Sciences*, 9(20), 4396. <https://doi.org/10.3390/app9204396>
- Ferrag, M. A., Maglaras, L., Moschogiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. <https://doi.org/10.1016/j.jisa.2019.102419>
- Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X., & Hamin, M. (2025). *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations* (NIST AI 100-2e2025). National Institute of Standards and Technology.
- Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE. <https://doi.org/10.1109/SFCS.1994.365700>
- Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5), 38–41. <https://doi.org/10.1109/MSP.2018.3761723>
- National Institute of Standards and Technology. (2024, August 13). *Announcing approval of three Federal Information Processing Standards (FIPS) for post-quantum cryptography*.
- National Institute of Standards and Technology. (n.d.). *Post-quantum cryptography*. NIST Computer Security Resource Center.
- European Union Agency for Cybersecurity. (2022). *Post-quantum cryptography: Anticipating threats and preparing the future*.
- Oktaviani, P. B., & Silvia, A. (2021). Strategi keamanan siber Malaysia. *Jurnal Kajian Ilmiah*, 21(1). <https://doi.org/10.31599/jki.v21i1.447>
- Recorded Future Inc. (2018). *Machine learning: Practical applications for cybersecurity*.
- Satrio, J., Maryam, S., Ummah, A., & Tri Saputra Wahidin, D. (2022). Peningkatan keterampilan keamanan siber bagi pengelola situs Desa Baros Kabupaten Serang. *Jurnal Inovasi Pengabdian dan Pemberdayaan Masyarakat*, 2(2). <https://doi.org/10.54082/jipm.35>
- Sigiro, F. H., Runturambi, A. J. S., & Widiawan, B. (2023). Collaborative sharing intelijen ancaman pada komunitas CSIRT dalam memperkuat keamanan siber nasional. *Syntax Literate: Jurnal Ilmiah Indonesia*, 7(9). <https://doi.org/10.36418/syntax-literate.v7i9.14245>
- Siska, M., Siregar, I., Saputra, A., Juliana, M., & Afifudin, M. T. (2023). Kecerdasan buatan dan big data dalam industri manufaktur: Sebuah tinjauan sistematis. *Nusantara Technology and Engineering Review*, 1(1). <https://doi.org/10.55732/nter.v1i1.1119>
- Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. *Jurnal Multidisiplin Indonesia*, 2(3). <https://doi.org/10.58344/jmi.v2i3.157>

Waskita, A. S., & Sidik, H. (2023). Diplomasi siber Indonesia dalam penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019. *Padjadjaran Journal of International Relations*, 5(2). <https://doi.org/10.24198/padjir.v5i2.41337>