TRANSPUBLIKA
Precise. Resilience. Felicitous.

Policy, Law, Notary and Regulatory Issues
https://ojs.transpublika.com/index.php/POLRI
Online ISSN 2809-896X

https://doi.org/10.55047/polri.v4i3.1761

Literature Review

The Urgency of Artificial Intelligence (AI) Technology Utilization in the Physical Security Sector: A Literature Review

Farid Alfarisi[1*], Surya Nita[2], Chairul Muriman Setiabudi[3]

[1-3]Police Science Study Program, School of Strategic and Global Studies, Universitas Indonesia, Depok, Indonesia
Email: [1)] faridalfaaa@gmail.com, [2)] suryanita.sksgui@gmail.com, [3)] cak_iir1966@yahoo.com

Received : 13 May - 2025
Accepted : 16 June - 2025
Published online : 20 June - 2025

Abstract

The increasing crime rate in Indonesia has led the public to question the effectiveness of the country's security systems, particularly physical security. This situation is further complicated by rapid technological advancements, which allow criminal acts to evolve in both motive and method. This article discusses the urgency of utilizing artificial intelligence (AI) technology in the physical security sector through a review of national and international literature. The literature analyzed in this study includes publications from the last ten years that are relevant to the topics of physical security and artificial intelligence. Key focus areas of this literature review include global trends in AI implementation in physical security, the benefits of its application, and the challenges faced during implementation. The findings reveal that the integration of AI, including the use of IoT devices, intelligent surveillance cameras, and biometric access control systems, can significantly improve the effectiveness of threat detection, prevention, and real-time response. However, in Indonesia, the application of AI in physical security remains limited due to infrastructure constraints, lack of human resource readiness, underdeveloped regulations, data privacy concerns, and high investment requirements. This study concludes that the application of AI in physical security is essential for enhancing safety, particularly in confined environments such as offices, residential areas, and commercial zones, in order to mitigate the rising trend of physical crimes.

Keywords: AI Security, Artificial Intelligence, Physical Security, Security Technology.

1. Introduction

Based on recent reports in the news media, criminal activities appear to persist without pause, occurring with growing regularity and escalating severity. According to the National Criminal Information Center (Pusiknas) of the Indonesian National Police's Criminal Investigation Agency (Bareskrim Polri), there were 25,350 cases of aggravated theft (Curat) in 2023, which was the highest among recorded crimes. This was followed by general theft with 21,225 cases and assault with 20,607 cases. Beyond the top three, motorcycle thefts were recorded at 9,231 cases in the same year (Pusiknas, 2024). These data indicate that theft remains the most prevalent crime across Indonesian society. This calls for urgent attention from law enforcement and related institutions to address these forms of physical crime.

Ranked tenth on the list is a newer form of crime that has emerged as a growing concern in light of the increasingly digital nature of technological developments. Data manipulation and electronic-based crimes (ITE) have also enabled perpetrators to commit theft, particularly the theft of personal data, which in many cases leads to further crimes such as unauthorized withdrawals from bank accounts and the misuse of data for online loan applications. These crimes represent an evolution of traditional physical crimes into digital-assisted acts.

The emergence of these new technology-driven crimes poses a new challenge to conventional physical security systems. Several developed countries have already begun incorporating AI technologies into their security industries, especially in the realm of physical security. Ryan Schonfeld, CEO of HiveWatch, a security technology firm, notes in an article for the Security Industry Association that AI can significantly improve the operational effectiveness of physical security systems (Schonfeld, 2025). For instance, AI-powered surveillance can detect and classify objects, individuals, and behaviors in real-time, alerting operators to potential threats instantly. Similarly, AI-based access control systems that use biometric recognition such as fingerprint and retina scanning have become part of modern security infrastructure (Septiyandini et al., 2024).

Despite these advances, AI implementation in Indonesia's physical security sector remains limited. Government institutions like the police and military, as well as private security companies and self-managed units (such as Satpam), have not fully adopted AI technologies in their operations. The main barriers include high investment costs, a lack of references and proven success cases, and insufficient human resource preparedness. According to Szymoniak et al. (2023), the application of AI in physical and environmental security systems can improve overall safety. Hanscomb (2024), in the Security Journal Americas, adds that AI, when combined with computational linguistics such as Large Language Models (LLMs), Natural Language Processing (NLP), and Large Vision Models (LVMs), can particularly enhance the effectiveness of surveillance systems within physical security. These techniques also play a key role in proactive physical security management (Olaoye & Egon, 2024). Given these perspectives, this research seeks to examine the urgency of adopting AI technologies to enhance physical security.

Although the implementation of artificial intelligence (AI) in physical security systems has been widely applied in developed countries, comprehensive studies focusing on its application in the Indonesian context are still very limited. Most previous studies have emphasized the cybersecurity aspect, while physical security, which is directly related to the protection of people and assets in the real world, has not been studied in relation to AI technology. In addition, not many studies have systematically reviewed the specific barriers faced by Indonesia, both in terms of infrastructure readiness, regulations, and human resources. The novelty of this research lies in filling the literature gap by presenting a review of recent literature that critically compares global trends and national conditions related to the application of AI in physical security, while highlighting the unique challenges faced by Indonesia.

This research aims to assess the urgency of utilizing artificial intelligence technology in the physical security sector in Indonesia through a national and international literature review approach within the last ten years. The main focus of this research is to identify global trends in the application of AI in physical security, evaluate the benefits it offers, and formulate the challenges that need to be overcome to realize effective integration of AI in Indonesia's physical security system. As such, this research is expected to provide a conceptual contribution to the development of AI implementation policies and strategies in the national security sector.

2. Methods

2.1. Research Methods

This study adopts a literature review method, in which the author collects and analyses journal publications, articles, and books that are relevant to the topic under discussion. The objective is to extract key insights, compare findings from each source, and identify gaps or limitations in the existing research (Creswell, 2019). In this article, the selected literature focuses on the application of artificial intelligence (AI) in physical security systems.

2.2. Data Source

The literature is gathered based on themes, research keywords, and article abstracts, then organized according to the level of relevance to the study's main objectives. The inclusion criteria for this research consist of publications, articles, and books published within the last ten years that focus specifically on physical security and artificial intelligence. The collected data are processed using thematic analysis and narrative synthesis.

2.3. Data Analysis Technique

The gathered data are analyzed using a thematic approach, in which each selected piece of literature is classified according to research variables, research methodology, and key findings. These elements are then synthesized into a narrative aligned with the main themes of the study, which include global trends in the use of AI in physical security, the benefits of AI implementation in physical security, and the challenges that may arise during its implementation in Indonesia.

3. Results and Discussion

3.1. Global Trends in the Use of Artificial Intelligence (AI) in Physical Security

Olaoye & Egon (2024) state that the integration of AI and machine learning technologies can significantly enhance physical security by combining data sources from Internet of Things (IoT) devices, surveillance cameras, and access control systems. This integration enables proactive threat detection and facilitates timely interventions. Similarly, Schonfeld (2025), a professional in the security technology sector, observes that many physical security systems in the United States now employ AI-supported technologies. These include surveillance cameras with facial recognition capabilities and access control systems equipped with alarm management based on real-time data processed by operators.

According to David L. Harris in a publication by ASIS International's Security Management, numerous companies across various industries in the U.S.—in the Fortune 1000 list—have adopted AI technologies to conduct comprehensive security data analysis. These companies have reported significant positive returns on investment (ROI) and emphasize the growing urgency to move beyond traditional surveillance systems and adopt more advanced AI-driven solutions (Harris, 2024). China, known for its rapid technological development, has implemented AI-based technologies in several of its smart cities, such as Shanghai and Hangzhou. These cities are equipped with advanced surveillance cameras, facial recognition systems, and data-driven city management platforms (Marvin et al., 2022). Moreover, AI-powered surveillance cameras capable of detecting crowd density were deployed during the Paris 2024 Olympics and are undergoing extended trials until March 2025, as reported by French news outlet Le Monde (Reynaud & Untersinger, 2024).

Such global trends suggest that the adoption of AI in physical security systems is not only technologically feasible, but also economically beneficial. These findings have a number of practical implications for Indonesia. First, policymakers need to invest in supporting infrastructure that enables data integration from various sources such as IoT, CCTV, and biometric systems to enable real-time analysis. Second, security companies need to prepare human resources through proper training in AI system operation and data interpretation to overcome resistance and skills gaps. Third, the regulatory framework should be adjusted to ensure the ethical use of AI, particularly in the context of the use of facial recognition and the protection of personal data, following concerns that have also been raised in the international context.

However, the implementation of AI in Indonesia potentially faces various challenges, such as limited digital infrastructure in remote areas, fragmented security data systems, and regulatory uncertainty. Therefore, strategic collaboration between the government, academia, and the private sector is crucial to initiate AI-based security system pilot projects in urban areas, which can then be developed in stages. The experiences of cities such as Shanghai and the Paris Olympics surveillance system initiative can serve as references in building a contextualized and scalable AI-based security model in Indonesia.

3.2. Benefits of AI Implementation in Physical Security

The concept of physical security, as described by Fennelly (2017) in Effective Physical Security, encompasses the policies, procedures, and technologies used to protect an area from unauthorized access, intrusion, or damage. This concept adopts a holistic approach and includes several core elements:

1) Deterrence

The meaning of deterrence within the concept of physical security refers to the visible presence of security measures intended to discourage potential intrusions or criminal activities.

2) Detection

Detection in this context may take the form of surveillance conducted within the secured area. This process is essential in supporting the physical security framework by facilitating both preventive measures and post-incident response. Detection can be carried out through various means, including the use of technological equipment such as CCTV systems, as well as security personnel conducting regular patrols.

3) Delay

In the context of physical security, delay mechanisms are implemented to prolong the time it takes for intruders attempting to commit direct criminal acts, such as theft, thereby hindering their ability to achieve their objectives swiftly.

4) Response

Through the implementation of preventive measures, early detection, and delay mechanisms against potential criminal actions by intruders or unauthorized individuals, it is essential to prepare appropriate response actions within the physical security system. Having a well-structured, prompt, and effective response plan constitutes a crucial component in reinforcing and complementing the preventive strategies already in place.

Based on this framework, it is evident that successful physical security requires coordination between human resources and technological support systems.

AI significantly enhances the effectiveness of threat detection and prevention (Masrichah, 2023). For instance, integrating deep learning techniques with CCTV systems has led to more advanced and efficient surveillance architectures (Hanscomb, 2024). Enhanced surveillance capabilities enable quicker and more comprehensive detection of threats through

facial recognition, crowd density analysis, and 24-hour monitoring. AI-integrated systems also enable proactive threat prevention through alarm management and access control based on real-time data processing, thus optimizing operational efficiency (Marvin et al., 2022; Olaoye & Egon, 2024; Szymoniak et al., 2023).

The implementation of AI reduces human error in security operations. Automated access control systems utilizing biometric technologies, multi-factor authentication (MFA), and continuous authentication (Dhanalakshmi et al., 2024; Pamarthy, 2025) not only enhance accuracy but also improve user experience. Biometric systems, for example, offer low false positive rates, while context-aware MFA optimizes security processes. In summary, AI contributes to increased efficiency, precision, and predictive capabilities, creating safer and more controlled environments (Campos et al., 2023).

Still, to encourage the successful implementation of AI in physical security systems in Indonesia, attention to several practical implications is needed. First, policymakers need to develop clear regulations on data protection, ethical use of AI, and operational standards for AI-based biometrics and surveillance systems. Second, investment in digital infrastructure is crucial, especially in areas that do not have adequate technological support. Partnerships between the government and the private sector can be an effective strategy in improving connectivity and technological readiness. Third, increasing the capacity of human resources is an absolute requirement through training and certification in managing AI-based security systems. Fourth, given the high cost of implementation, the provision of fiscal incentives or financial support needs to be considered so that small and medium-scale businesses can gradually adopt this system. Finally, ethical aspects and social acceptance must also be considered. The government and technology providers need to prioritize transparency and involve the public in policy formulation to build public trust in AI-based surveillance systems.

Thus, while AI offers various benefits in strengthening physical security systems, its success in Indonesia is highly dependent on the synergy between adaptive regulations, infrastructure readiness, human resource capacity building, and inclusive community participation. A strategic and targeted approach will ensure that AI technology not only enhances security, but also aligns with Indonesia's legal, social, and ethical values.

3.3. Implementation Challenges in Indonesia

In Indonesia, AI is more commonly applied in cybersecurity for protecting information and data, while its use in physical security remains limited. A notable example of successful AI implementation in physical security is the Automatic License Plate Recognition (ALPR) system used by the Indonesian National Police (Polri) as part of its Electronic Traffic Law Enforcement (ETLE) initiative. However, deploying such systems nationwide requires advanced and evenly distributed technological infrastructure. Several studies have identified the following challenges to AI adoption in Indonesia's physical security sector:

1) Inadequate and uneven technological infrastructure (Pradana et al., 2025; Syarifudin, 2024).
2) Limited availability of skilled and trained human resources with adequate technological awareness (Pradana et al., 2025; Herawati et al., 2023).
3) Regulatory frameworks that are not yet supportive of AI development and implementation (Herawati et al., 2023; Pradana et al., 2025).
4) Concerns regarding data privacy and security (Pradana et al., 2025; Syarifudin, 2024; Szymoniak et al., 2023).
5) High investment requirements for equipment, training, and public outreach (Hanscomb, 2024; Olaoye & Egon, 2024; Szymoniak et al., 2023).

To address these challenges and encourage wider adoption of AI in physical security, there are a number of practical recommendations that can serve as a reference for policymakers, security agencies, and other stakeholders. First, there is a need for comprehensive regulatory reform so that the existing legal framework can accommodate the safe, ethical, and responsible use of AI, including the protection of personal data and clarity of legal liability. Second, digital infrastructure development needs to be accelerated through collaboration between the public and private sectors, especially to reach technologically disadvantaged areas. Third, human resource capacity building is prioritized through technical training, certification, and integration of AI curriculum in vocational and higher education.

It is also important to increase public trust in AI systems through educational campaigns that socialize the benefits, functions, and legal protections attached to this technology. Finally, the government can encourage private sector involvement through fiscal incentives such as subsidies or tax deductions for companies that develop or implement AI technology in physical security systems. With this strategic approach, Indonesia has the opportunity to overcome existing structural barriers and optimize the potential of AI as an adaptive and sustainable future security solution.

4. Conclusion

The integration of artificial intelligence into physical security systems can significantly enhance overall effectiveness and safety, provided that its technological capabilities are maximized. AI can improve the speed of threat detection, surveillance accuracy, and operational efficiency. However, the implementation of AI-based security systems also presents several challenges. These include the necessity for adequate infrastructure and skilled human resources capable of operating such advanced technologies. Concerns regarding data privacy and security remain substantial, especially considering Indonesia's ongoing struggle with data breaches. Furthermore, the substantial investment costs required for equipment procurement, socialization, and training must also be taken into careful consideration.

Based on the findings of this study, which analyzes various national and international sources, it can be concluded that while the use of AI in physical security is both relevant and important, its application is currently more feasible in limited environments such as office complexes, residential areas, warehouses, and commercial zones. This targeted approach could contribute to a reduction in the number of physical crimes, which remain a pressing issue in Indonesia.

5. References

Campos, J. E. M. R., Rodríguez, C. S. C., Luján, L. D. A., & Santos, A. C. M. de los. (2023). Sistema de reconocimiento facial para el control de accesos mediante Inteligencia Artificial. *Innovación y Software*, *4*(1), 24–36. https://doi.org/10.48168/innosoft.s11.a78

Creswell, J. W. (2019). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications, Inc.

Dhanalakshmi, S., Priyadharshini, M., Saranya, G., Haripriya, P. S., & Kavitha, K. (2024). AI-Enhanced Access Control and Authentication. *Journal of Cyber Security in Computer System*, *3*(3).

Fennelly, L. J. (2017). *Effective physical security*. Elsevier Inc.

Hanscomb, V. (2024). *How AI architectures are transforming physical security*. SJA Security Journal Americas.

Harris, D. L. (2024). *A Force Multiplier: Why Physical Security Teams Should Leverage AI*. ASIS International.

Herawati, A. R., Widowati, W., & Maesaroh, M. (2023). The Implementation of Artificial Intelligence in Indonesia's Public Service: Challenges and Government Strategies. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, 2471–2480. https://doi.org/10.46254/AU01.20220537

Marvin, S., While, A., Chen, B., & Kovacic, M. (2022). Urban AI in China: Social control or hyper-capitalist development in the post-smart city? *Frontiers in Sustainable Cities*, *4*(3), 308–318. https://doi.org/10.3389/frsc.2022.1030318

Masrichah, S. (2023). Ancaman Dan Peluang Artificial Intelligence (AI). *Khatulistiwa: Jurnal Pendidikan Dan Sosial Humaniora*, *3*(3), 83–101. https://doi.org/10.55606/khatulistiwa.v3i3.1860

Olaoye, F., & Egon, A. (2024). Real-time Predictive Analytics for Physical Security. *Security Informatics*.

Pamarthy, S. K. (2025). AI-Powered Risk-Based Access Control: Advanced Security Framework for Modern Systems. *International Journal of Research in Computer Applications and Information Technology*, *8*(1), 3031–3045. https://doi.org/10.34218/IJRCAIT_08_01_219

Pradana, A. E., Herawati, A. R., Dwimawanti, I. H., & Maesaroh. (2025). Tantangan Kecerdasan Buatan Dalam Implikasi Kebijakan Pemerintah di Indonesia: Studi Literatur. *Jurnal Good Governance*, 51–66. https://doi.org/10.32834/gg.v21i1.889

Pusiknas. (2024). *Curat, Kejahatan Paling Sering Terjadi di 2024*. Pusiknas Bareskrim Polri.

Reynaud, F., & Untersinger, M. (2024). *Paris 2024: Controversial AI-led video surveillance put to the test during Olympics*. La Monde.

Schonfeld, R. (2025). *Transforming Physical Security: How AI is Changing the GSOC*. Security Industry Association. https://www.securityindustry.org/2025/03/03/transforming-physical-security-how-ai-is-changing-the-gsoc/

Septiyandini, W., Muriman, C., & Mayastinasari, V. (2024). The Impact of Artificial Intelligence (AI) on Human Resources: A Case Study of the Indonesian Police Institution. *POLICY, LAW, NOTARY AND REGULATORY ISSUES*, *4*(1), 64–74. https://doi.org/10.55047/polri.v4i1.1540

Syarifudin, A. S. (2024). Challenges and Opportunities for the Application of AI in Language Learning in Indonesia. *Transformational Language Literature and Technology Overview in Learning (Transtool)*, *3*(1), 49–60. https://doi.org/10.55047/transtool.v3i1.1351

Szymoniak, S., Depta, F., Karbowiak, Ł., & Kubanek, M. (2023). Trustworthy Artificial Intelligence Methods for Users' Physical and Environmental Security: A Comprehensive Review. In *Applied Sciences (Switzerland)* (Vol. 13, Issue 21). https://doi.org/10.3390/app132112068