JURNAL RESISTOR | ISSN 2598-7542 | E-ISSN 2598-9650
Vol. 3 No 1 – April 2020 | https://s.id/jurnalresistor
DOI: https://doi.org/10.31598
Publishing: Prahasta Publisher

Analysis of Physical Security and Comprehensive Approach Based on Artificial Intelligence Method

Siti Alvi Sholikhatin[1], Alif Nur Fadilah[2], Rashif Syaddad[3]

[1 3] Digital Business, Faculty of Business and Social Studies, Amikom Purwokerto University
Purwokerto, Indonesia
[2] Informatics, Faculty of Computer Studies Amikom Purwokerto University
Purwokerto, Indonesia

e-mail: sitialvi@amikompurwokerto.ac.id[1] , alifnurfadilah484@gmail.com[2]
,rashifsyaddad518@gmail.com[3]

Received : March, 2025	Accepted : April, 2025	Published : April, 2025

Abstract

Cybersecurity sets as an emerging issue in the recent years, in line with the development of increasingly sophisticated digital technology. Cybersecurity are divided into several areas that are equally important and interconnected to one another. One of the areas of cybersecurity is physical security. Physical security involves safeguarding personnel, hardware, software, networks, and data against physical actions and incidents that may lead to significant loss or harm to an organization, agency, or institution. Several methods are conducted to secure the area physical assets, and AI-based method is currently well-known for its effectiveness. In this research, we aim to proposed an AI-based method to improve the physical security. This research is conducted to analyze and propose a method in the area of physical security. The goals are to secure the physical assets, predict potential attacks, and manage the vulnerable risks. The results of this research are the proposed prototype to secure physical area of information system and able to detect unusual activities to prevent incident that can be harmful of physical sources.

Keywords: *Physical security, Artificial intelligence, Cybersecurity, Information security*

Abstrak

Keamanan siber menjadi isu yang berkembang dalam beberapa tahun terakhir, seiring dengan perkembangan teknologi digital yang semakin canggih. Keamanan siber dibagi menjadi beberapa area yang sama pentingnya dan saling berhubungan satu sama lain. Salah satu area keamanan siber adalah keamanan fisik. Keamanan fisik adalah perlindungan personel, perangkat keras, perangkat lunak, jaringan, dan data dari tindakan dan kejadian fisik yang dapat menyebabkan kerugian atau kerusakan serius pada suatu perusahaan, instansi, atau lembaga. Beberapa metode dilakukan untuk mengamankan aset fisik area, dan metode berbasis AI saat ini terkenal dengan keefektifannya. Dalam penelitian ini, kami bertujuan untuk mengusulkan metode berbasis AI untuk meningkatkan keamanan

fisik. Penelitian ini dilakukan untuk menganalisis dan mengusulkan sebuah metode di bidang keamanan fisik. Tujuannya adalah untuk mengamankan aset fisik, memprediksi potensi serangan, dan mengelola risiko yang rentan. Hasil dari penelitian ini adalah prototipe yang diusulkan untuk mengamankan area fisik sistem informasi dan mampu mendeteksi aktivitas yang tidak biasa untuk mencegah insiden yang dapat membahayakan sumber fisik.

Kata Kunci: *Keamanan fisik, Kecerdasan buatan, Keamanan siber, Keamanan informasi*

1. INTRODUCTION

In the recent years, according to DataIndonesia.id, BSSN recorded that Indonesia received 370.02 million cyber attacks in 2022 [1]. This number increased by 38.72% from the previous year, which amounted to 266.74 million cyberattacks. Cybersecurity need to be addressed seriously in order to ensure that Indonesia is secure from cyber attacks. Cybersecurity have been evolving rapidly, but unfortunately, cybercriminals are also using updated technology to launch increasingly sophisticated cyberattacks while hiding their tracks [2]. Cybersecurity are divided into several field: network security, physical security, and computer security. These areas are interconnected and equally important in the system. The cybersecurity system is defined as a set of processes, human beings and systems which assist in the protection of electronic resources.

Artificial intelligence is an idea that mirrors human cerebrum and seeks to explore realworld issues in a holistic way. Artificial intelligence, which provides tools to solve complex and stressful problems, can be described as performance technology. Artificial intelligence is a combination of data innovation and physical intelligence that can be used electronically to achieve the objectives. AI-based system has been developed in many areas to make life easier for humans. In the area of cybersecurity, AI can be developed to detect threat, predict the security risks, and even prevent attacks. Artificial intelligence does not only pose threats and dangers, it can also be used to solve problems. Information flow and operational direction are used to detect, prevent and identify cyber-attacks [3].

The research conducted by Sarvesh Kumar [4] stated that AI innovation is playing an progressively imperative part in driving computerization in cyber security. By mechanizing numerous of the schedule and unremarkable errands related with cyber security, AI empowers security work force to center on more key viewpoints of their work, such as danger examination and occurrence reaction. One range where AI is having a critical affect is within the computerization of danger location. Utilizing progressed machine learning calculations, AI-powered apparatuses can naturally examine tremendous sums of information to identify potential security dangers. This will offer assistance security groups rapidly identify and react to developing dangers, decreasing the hazard of an effective cyberattack. In expansion to danger discovery, AI is additionally being utilized to robotize other perspectives of cybersecurity, such as occurrence reaction and vulnerability administration. For illustration, AI-powered devices can consequently examine security episodes to decide the foremost fitting reaction, or consequently check frameworks for vulnerabilities and propose remediation activities.

The following research is conducted by Yao Jun [5] indicates that an assessment of IoT advancements involves examining characteristics, structures, applications, facilitating technologies, and upcoming challenges related to technological upgrades. The research has also examined the structure of the IoTs, which comprises the perception layer, transmission layer, application layer, and network management. Furthermore, it examines the facilitating technologies of the IoTs, which encompass application domain, middleware domain, network domain, and object domain. This research has examined the function of IoTs and their usage in people's daily lives through the creation of smart cities, smart agriculture, waste management, retail and logistics, as well as a smart environment.

The third research is conducted by Meraj Farheen Ansari [6] shows that while AI helps the security team save time, it still needs human experts for creative tasks, thereby simplifying their work. The restriction requires developers to ensure that the technology is

endowed with various functions to manage any crime arising from their limitations.

This study aims to examine and suggest a technique within the field of physical security. The goals are to secure the physical assets, predict potential attacks, and manage the vulnerable risks. The object of this research is university X that currently experienced fire in information system physical assets. The incident caused huge losses, loss of critical data assets, and caused delays in several academic activities involving the system.

2. RESEARCH METHOD

The flow of this research can be seen in the flow chart Figure 1.

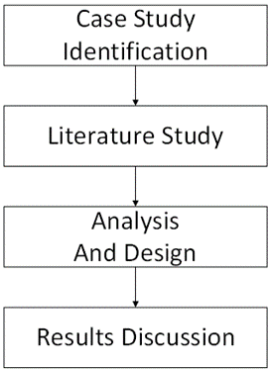

Figure 1. Research flow

a. Case study identification
   The first step of this research is to identify the case in university X. The researcher conducted thorough investigation and observation to understand the overall problems.
b. Literature study
   The approach used in this research is based on artificial intelligence method. In cyber defense or cybersecurity, there are several methods that can be used, so we attempt to propose an AI-based method in order to secure physical assets in cybersecurity.
c. Analysis and design
   Analysis is the step to assess the findings in the first method and then design the method that best fit to implement in the physical security. This step may need several trials in order to make sure that the method is highly beneficial. The result of this design is a prototype that need to be evaluated for the next implementation process.
d. Results discussion
   The last step is to discuss the analysis results and evaluate the overall research stages.

3. RESULT AND DISCUSSION

3.1 Case study identification

The incident of physical security occurred at university X in early 2024. The fire has burned half of the infrastructure in the server building and cause damaged not only to the physical assets but also data assets. From the assessment conducted after the fire, it is found that the department have not implemented the security standard, for example, ISO 27001 to secure the information system.

3.2 Literature Study

The research conducted by [7], shows advanced testing of physical security systems through AI/ML. The research proposed a through ways of secure the physical area with these steps:

1. Optimization methods for low level tasks
   a. Sensor placement for maximum area coverage
   b. Sensor selection to minimize false alarms
   c. Randomization of guard routes
   d. Mechanical engineering analysis for materials selection of walls and fences
2. More advanced
   a. Facility layout with Adversary Sequence Diagrams
   b. Simulation of force on force interactions

The proposed technique is shown below in Figure 2.

The research conducted by [8], shows different AI methods and tools for intelligent security privacy safeguarding. In addition, unresolved problems and challenges concerning AI-driven SC are examined. Ultimately, a retail marketing case study is showcased that employs AI and intelligent security to maintain its safety and confidentiality.

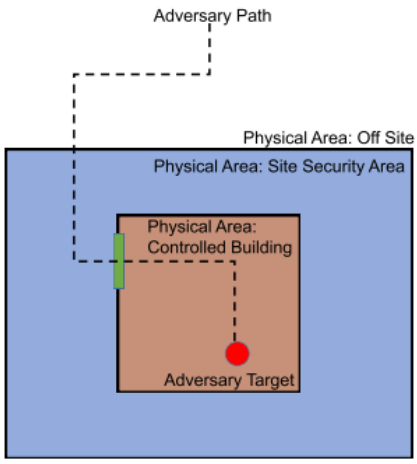

Figure 2. Physical Security with ML
[Source: [7]]

The research conducted by [9], shows there could be cybersecurity threats when standard vulnerable Industrial Control System (ICS) settings implement Industry 4.0. For example, if AI is utilized to manage the ICS autonomously, there is a danger that attackers could compromise ICS by targeting AI through methods like dataset pollution. It could damage both physical and logical assets, thus it is recommended to implement various countermeasures for ICS and associated systems like AI to mitigate cyber risk.

The research conducted by [10], the experimental results demonstrate the vulnerability of the LSTM, cLSTM, biLSTM, and CNN models to adversarial attacks. The MSE values achieved through different attack techniques and epsilon values underscore the models' vulnerability to adversarial changes. Greater MSE values suggest a larger divergence from the anticipated outputs and highlight a more substantial effect of the attacks on the models' forecasts. The results indicate that the reliability of the models differs based on various attack techniques and epsilon parameters.

The research conducted by [11], the study has effectively performed an extensive security risk evaluation employing the OCTAVE Allegro approach and has recognized 10 essential cyber and physical assets. The research findings reveal that around 15 security threats arise from both internal and external factors associated with smart homes. The effects or outcomes of these risks have been outlined, presuming that the dangers materialize. Proposed measures to reduce the risks to an acceptable level have been deemed suitable. This research has concentrated exclusively on identifying security threats, impacts or risks, along with appropriate countermeasures for smart homes based on IoT technology.

The research conducted by [12], the paper proposes a structure that AI-CPS applies. The core approach of the suggested system is to create multiple classifiers and train each one separately. A network viewpoint acknowledges the wider challenges and connections between surveillance and security measures by focusing on how organizations work together, interact, and coordinate. Studying and putting in place countermeasures is an urgent necessity for sports stadiums or arenas to safeguard their sensitive data from being compromised by unauthorized sources. Network protection based on cyber-physical systems has become crucial for maintaining a business's confidentiality, as it stops unauthorized individuals from accessing network systems, guarantees safe direct transmission of sensitive data, and provides a strong alert mechanism for warnings and security breaches. This research examines various threats and assaults on network systems along with the typical countermeasures to mitigate the issue.

The research conducted by [13], the paper reviews the state of the art approaches covering different kinds of Cyber Physical Systems (CPS) and different means of security analysis using machine learning approaches and deep learning as well. There are different attacks found in the literature that need to be dealt with in a CPS. They include replay attack, DoS attack, jamming attacks, time synchronization attack, stealth time synchronization attack, false data injection attack and so on.

The research conducted by [14], The main goal of this work was to utilize AI and ML techniques to enable the early identification of cyber-attacks targeting the physical system. We researched and analyzed several different strategies for initiating a cyberattack. In recent years, methods for initiating cyberattacks have experienced a significant evolution. Since individuals who engage in cybercrime are constantly developing new methods to bypass security protocols, there remains an ongoing

demand for innovative detection systems. Due to the extensive information that had to be gathered from several diverse sources, identifying cyber attackers required utilizing methods from both AI and ML. We introduce a Fuzzy Logic Hidden Markov Model (SFL-HMM) that relies on Heuristic Multiple Swarm Optimization to detect malicious cyber behavior (HMS-ACO).

The research conducted by [15], a lightweight authentication protocol aided by AI in industrial medical Cyber Physical Security (CPS) utilizing a Chebyshev map was suggested to fulfill the need for real-time access. Incorporating the Chebyshev map into the lightweight authentication protocol ensures the safety of sessions and the confidentiality of patients' information. The proposed model shown in the Figure 3 below.

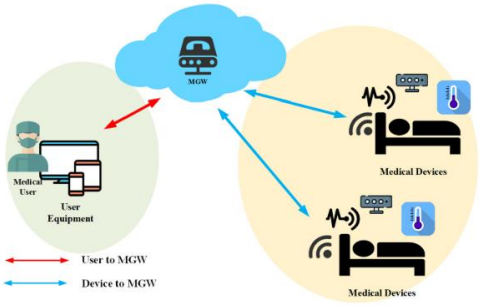

Figure 3. Introduction Model
[Source: [15]]

The research conduted by [16], the paper reviewed various authentication schemes, blockchain-based IoT authentication frameworks, Artificial Intelligence-driven smart decisive learning authen- tication models. Also, the article offered a comparative examination of several currently available studies important in IoT security from a traditional, blockchain, and AI viewpoint. This article concludes with the hope that upcoming authentication methods and key management solutions will effectively tackle these challenges.

3.3 Analysis and Design

Based on the assessment of the physical environment of the system infrastructure, we proposed the prototype of physical security based on AI approach, shown in Figure 4 below.

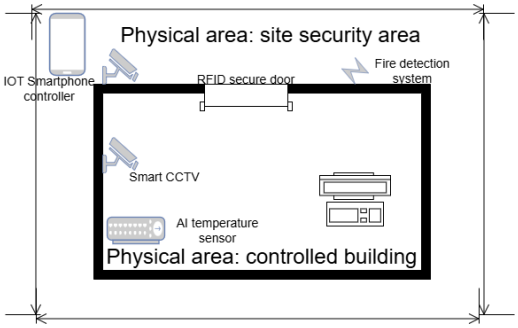

Figure 4. Physical Security Area based on AI Approach

Physical security system on AI-based approach consists of two environments:

1. Site security area or external environment
   External environment consists of RFID secure door as an access control. This is very basic security to allow only authority who can access. Biometric authentication and card identification double up the protection. Closed-Circuit Television (CCTV) implemented in both areas, and are connected to IoT based smartphone. This can ensure fully-monitored devices on both areas. The CCTVs are also regularly backing up every week. Fire detection system implemented in external environment to prevent potential danger especially fire and other hot sources.
2. Controlled building or internal environment.
   Controlled building consists of AI-based temperature sensor for early detection. The sensor is modified into smart sensor so it can reduce temperature automatically if the sensor if above threshold value. Electrical stabilizer also implemented to prevent unstable voltage. Because from the recent incident, it is predicted that the fire is caused by the electrical short circuit. The CCTV placed in the internal environment is connected to the IOT based smarphone to make sure 24/7 monitor.
3. CCTV logs are being stored and collected regularly, the data is used in machine learning to idetify suspicious movements such as: unclear back and forth steps, the presence of an object covering the face or head, unknown access in the secure door, and weird noises that are too low or too loud made in the are. The data is learned to predict attempts to break into the secure area.

3.4 Results

The results of the research are the prototype that later would be implemented in the physical security site. The prototype is still in the form of simulation and proposed idea, in-depth evaluation is required for this prototype to be implemented in an actual environment. University x is currently undergoing the full assessment of information security, and physical security is one of the most important aspect to be secured. AI-based tools are implemented in both external and internal area of physical infrastructure. These tools are expected to detect potential rise of temperature or unstable electrical activity in the internal building.

4. CONCLUSION

This research aims to develop a methodology for improving physical security by securing assets, predicting potential attacks, and managing vulnerabilities. The study focuses on University X, which recently experienced a fire that caused significant damage to information system assets, loss of critical data, and academic delays. The proposed physical security system has two key components: the external environment (site security) and the internal environment (controlled building).

In the external environment, RFID-secured doors control access, allowing only authorized individuals to enter. Additional protection is provided by biometric authentication and card identification. CCTV cameras monitor both environments and are connected to IoT-based smartphones for continuous surveillance, with weekly backups of footage. A fire detection system is also implemented externally to detect potential hazards like fires.

In the internal environment, AI-based temperature sensors detect overheating and automatically reduce the temperature if it exceeds the threshold. An electrical stabilizer is also installed to prevent voltage fluctuations, addressing the fire hazard caused by a recent electrical short circuit. CCTV in this area is also connected to IoT-based smartphones for 24/7 monitoring, ensuring constant vigilance.

STATEMENT OF APPRECIATION

The authors would like to thank Department of Research and Service Community of Amikom Purwokerto University for their support and additional funding regarding this paper.

REFERENCES

[1] DataIndonesia.id, "BSSN Catat 370,02 Juta Serangan Siber ke Indonesia pada 2022," 2023. https://dataindonesia.id/internet/detail/bssn-catat-37002-juta-serangan-siber-ke-indonesia-pada-2022 (accessed Feb. 26, 2024).

[2] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.

[3] J. Jain, "Artificial intelligence in the cyber security environment," *Artif. Intell. Data Min. Approaches Secur. Fram.*, pp. 101–117, 2021, doi: 10.1002/9781119760429.ch6.

[4] S. Kumar, U. Gupta, A. K. Singh, and A. K. Singh, "Artificial Intelligence: Revolutionizing cyber security in the Digital Era," *J. Comput. Mech. Manag.*, vol. 2, no. 3, pp. 31–42, 2023, doi: 10.57159/gadl.jcmm.2.3.23064.31.

[5] Y. Jun, A. Craig, W. Shafik, and L. Sharif, "Artificial Intelligence Application in Cybersecurity and Cyberdefense," *Wirel. Commun. Mob. Comput.*, vol. 2021, 2021, doi: 10.1155/2021/3329581.

[6] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review," *Ijarcce*, vol. 11, no. 9, pp. 81–90, 2022, doi: 10.17148/ijarcce.2022.11912.

[7] P. Durko, "Advanced Testing of Physical Security Systems through AI/ML," 2021, doi: 10.2172/1831133.

[8] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges," *IEEE Access*, vol. 8, pp. 24746–24772, 2020, doi: 10.1109/ACCESS.2020.2970576.

[9] W. Matsuda, M. Fujimoto, T. Aoyama, and T. Mitsunaga, "Cyber Security Risk Assessment on Industry 4.0 using ICS

testbed with AI and Cloud," *2019 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2019*, pp. 54–59, 2019, doi: 10.1109/AINS47559.2019.8968698.

[10] U. Cali, F. O. Catak, and U. Halden, *Trustworthy cyber-physical power systems using AI: dueling algorithms for PMU anomaly detection and cybersecurity*, vol. 57, no. 7. Springer Netherlands, 2024. doi: 10.1007/s10462-024-10827-x.

[11] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors (Switzerland)*, vol. 18, no. 3, pp. 1–17, 2018, doi: 10.3390/s18030817.

[12] B. Wan, C. Xu, R. P. Mahapatra, and P. Selvaraj, "Understanding the Cyber-Physical System in International Stadiums for Security in the Network from Cyber-Attacks and Adversaries using AI," *Wirel. Pers. Commun.*, vol. 127, no. 2, pp. 1207–1224, 2022, doi: 10.1007/s11277-021-08573-2.

[13] A. Ahmed Jamal, A. A. Mustafa Majid, A. Konev, T. Kosachenko, and A. Shelupanov, "A review on security analysis of cyber physical systems using Machine learning," *Mater. Today Proc.*, vol. 80, no. xxxx, pp. 2302–2306, 2023, doi: 10.1016/j.matpr.2021.06.320.

[14] R. Almajed, A. Ibrahim, A. Z. Abualkishik, N. Mourad, and F. A. Almansour, "Using machine learning algorithm for detection of cyber-attacks in cyber physical systems," *Period. Eng. Nat. Sci.*, vol. 10, no. 3, pp. 261–275, 2022, doi: 10.21533/pen.v10i3.3035.

[15] R. Qi, S. Ji, J. Shen, P. Vijayakumar, and N. Kumar, "Security preservation in industrial medical CPS using Chebyshev map: An AI approach," *Futur. Gener. Comput. Syst.*, vol. 122, pp. 52–62, 2021, doi: 10.1016/j.future.2021.03.008.

[16] A. Attkan and V. Ranga, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex Intell. Syst.*, vol. 8, no. 4, pp. 3559–3591, 2022, doi: 10.1007/s40747-022-00667-z.