Utilizing Machine Learning for Anomaly Detection in Cybersecurity Systems

Budi Utami Fahnun[1], Eel Susilowati[2], Hadyan Mardhi Fadlillah[3], Irawaty[4]
[1,2,3,4]Universitas Gunadarma, Indonesia
Email: bufahnun@staff.gunadarma.ac.id

Abstract

Anomalies in cybersecurity systems are increasingly complex and sophisticated, making detection difficult using traditional rule-based and signature-based approaches. In facing these challenges, machine learning is crucial to improve real-time anomaly detection capabilities. This study aims to explore the role of machine learning in detecting anomalies in cybersecurity systems. The research method is carried out using a qualitative approach, collecting data from relevant literature and interviews with experts in the fields of cybersecurity and machine learning. The results of this study indicate that machine learning can effectively improve the ability of cybersecurity systems to detect and respond to threats more quickly and accurately. Implementing machine learning allows for deeper analysis of complex cybersecurity data, recognizing unexpected anomalous patterns, and adapting to new attacks. Despite challenges such as data variability and dynamic operational environments, the evaluation of model performance shows significant progress in protecting information systems from increasingly complex threats. The future of anomaly detection in cybersecurity promises the possibility of developing more sophisticated technologies, strengthening defenses against evolving threats, and improving overall security.

Keywords: *Machine Learning, Anomaly, Cybersecurity System.*

A. INTRODUCTION

Cybersecurity has become one of the most critical aspects of this digital era, given the significant increase in increasingly sophisticated and destructive cyberattacks. Cybersecurity systems aim to protect data, networks, programs, and devices from unwanted attacks. However, with the increasing complexity of technology and attack methods used by cybercriminals, the challenge of maintaining the security of information systems is also increasing. Many organizations, both public and private sectors, face very high risks if their security measures are inadequate (Djenna et al., 2021). As information technology advances, the amount of data generated by digital activities is also increasing exponentially. This large volume of data, which often contains complex and irregular patterns, creates additional challenges for traditional security systems that are often unable to identify hidden threats or anomalies in the data. This is where machine learning technology plays a vital role. Machine learning allows systems to learn from historical data and recognize patterns or anomalies that may indicate the presence of a cyber threat (Sturgeon, 2021).

Over the past few decades, researchers and practitioners have worked hard to develop various methods to improve threat detection in cybersecurity. Traditional rule-based and signature-based techniques are often inadequate in dealing with new

attacks that do not yet have known signatures. Therefore, anomaly-based approaches powered by machine learning offer a promising alternative because they can detect unusual or suspicious behavior that may indicate an attack (Kaur et al., 2023). Machine learning has been widely used in a variety of technology applications, from facial recognition to sentiment analysis in social media. In the context of cybersecurity, machine learning has great potential to detect anomalies that traditional methods might miss. By analyzing network traffic data, system logs, and other data sources, machine learning algorithms can identify suspicious or unusual patterns that may indicate a cyberattack (Balaji et al., 2021).

The main challenges in applying machine learning for anomaly detection are the need for high-quality, representative data, and the ability to adjust the model to adapt to new and evolving attack patterns. In addition, model interpretability is also an important factor, as understanding why an anomaly was detected is critical for appropriate mitigation measures. Nonetheless, the advantages offered by machine learning in improving cybersecurity make it a very interesting and relevant topic for further research (Al-amri et al., 2021). The rise of digital infrastructure and the adoption of the Internet of Things (IoT) technology are further expanding the attack surface that must be secured. Every device connected to a network is a potential entry point for cyberattacks. Machine learning can help identify anomalies in the data generated by IoT devices, which are often scattered and varied in form and volume. Thus, integrating machine learning into cybersecurity strategies can help improve protection against evolving threats (Omolara et al., 2022).

In an era where data is a very valuable asset, protecting the integrity and confidentiality of data is a top priority for many organizations. Cyberattacks not only cause huge financial losses but can also damage reputation and customer trust. Therefore, investing in technologies that can improve the ability to detect and respond to cyber threats is a very strategic step (Pandey et al., 2020). By leveraging the analytical power of machine learning, it is expected to achieve significant improvements in the effectiveness of cybersecurity systems, thereby protecting data and digital assets from increasingly complex and dangerous threats. This research aims to address these challenges by developing models and techniques that can detect anomalies more effectively, making a valuable contribution to the field of cybersecurity.

B. LITERATURE REVIEW

1. Machine Learning

Machine learning refers to a method that gives computers the ability to learn and do a job automatically. The machine learning process is carried out through a certain algorithm so that the work order to the computer can be done automatically. Machine learning is carried out through 2 phases, namely the training phase and the application phase. The training phase is the modeling process of the algorithm used will be learned by the system through training data, while the application phase is the modeling process that has been learned by the system through the training phase and will be used to produce a certain decision, using testing data (Taye, 2023).

Machine learning can be done in two ways, namely supervised learning and unsupervised learning. Unsupervised learning is the processing of sample data carried out without requiring the final result to have a form that matches a certain form, using several sample data at once. The application of unsupervised learning can be found in the visualization process, or data exploration. Supervised learning is the processing of sample data x will be processed in such a way that it produces output that matches the final result y. Supervised learning can be applied to the classification process (Rahmani et al., 2021).

The learning process begins with observations or data, such as examples, direct experience, or instructions, to find patterns in the data and make better decisions in the future based on the examples given. The main goal is to allow computers to learn automatically without human intervention or assistance and adjust their actions accordingly (Smith et al., 2022). Some methods of Machine Learning:

a) Supervised Machine Learning
   The algorithm takes a set of examples as input (called training examples), then each training class has a certain label that can be recognized and has a set of features associated with the values. The model then displays or predicts the class of new examples by giving the feature values, the results are associated with a certain sensitivity (called accuracy in information science) (Dong, 2021). A feature extractor is used to convert each input value to a feature set. This feature set, which captures basic information about each input that should be used to classify it, the pair of feature sets and labels is fed into the machine learning algorithm to produce a model. During prediction, the same feature extractor is used to convert the unknown input to a feature set. This feature set is then fed into the model, which then produces the predicted label (Omuya et al., 2021).
b) Unsupervised Machine Learning
   Studying how unsupervised learning systems can infer a function to describe the hidden structure of unlabeled data. Reasons for using this type of tool may be because the class for the instance is unknown, historical data for training the algorithm is not available, or the user may want to explore new classifications for the data. The system does not know the exact output but explores the data and can draw conclusions from the dataset to describe the hidden structure of the unlabeled data (Vercio et al., 2020).
c) Reinforcement Machine Learning
   Machine Learning is where the agent learns something by performing certain actions and seeing the results of those actions (learning based on the experience experienced by the agent). So Reinforcement Learning is based on the interaction of the agent executing the action and its environment which provides positive or negative feedback, such as rewards. In Reinforcement Learning (RL), the learning process can be described as a loop where:
   1) The agent receives a State (S0) from the existing Environment.
   2) Based on the State (S0), the agent will act (A0).
   3) The Environment will change to a new State (S1).

4) The Environment will provide a 'Reward' (R1) to the agent (Akalin & Loutfi, 2021).

The process will be repeated, the aim of which is for the agent to maximize the cumulative reward obtained

Machine learning enables the analysis of large amounts of data. Machine learning generally provides faster, more accurate results to identify profitable opportunities or dangerous risks, but it may also require additional time and resources to properly train the machine learning. Machine learning combined with cognitive technologies can make the job more effective in processing large volumes of information (Sujith et al., 2022).

2. Cyber Security

Cybersecurity refers to the activity, process, capability ability, or position in which information and communication systems and the information stored therein are protected from damage, use, modification, or exploitation by unauthorized parties. Users who use information without the ability to use cybersecurity tools are considered to have violated information security. In a cybersecurity system, information protection efforts are carried out at locations that have the greatest potential for the greatest gaps in experiencing cybercrime or attacks (Turk et al., 2022).

In cybersecurity protection, cybersecurity skills are increasingly needed along with the increasing trend of cybercrime or attacks in various organizations. This cybersecurity protection is directed at protecting the information technology devices they have so that these devices are protected from malware attacks and data breaches. Malware is malicious software designed to harm, infiltrate, or damage computer systems with certain codes where the victim is not immediately aware of the attack on their computer system (Trim & Lee, 2021). Meanwhile, data theft generally occurs in companies and these cybersecurity crimes or attacks represent the greatest cybersecurity risk to the organization's reputation, not just to the company's financial losses. Privacy Rights Clearinghouse reports that more than 607 million data have been lost or stolen from approximately 3,500 data breaches. This cybersecurity risk occurs in various companies because cybersecurity experts or engineers are unable to properly handle the data theft issues (Corallo et al., 2020).

According to Defense Law Number 3 of 2002, threats to the national defense system include military and non-military threats, including cyber threats. Cyberthreat is defined as an action, disruption, or attack that can damage or affect a system by threatening its confidentiality, integrity, and availability. Assessing a cyber defense organization requires an understanding of the various threats and attacks in cyberspace and how to evaluate the potential risks associated with them. Therefore, determining the potential threats and attacks in cyberspace contributes to determining procedures and strategies to evaluate the effectiveness of a cyber defense organization in combating and limiting the impact of these threats and attacks (Klenka, 2021).

By definition, a cyber threat is a potential danger that is believed to cause harm, disruption, or attack to information security, namely the confidentiality, integrity, and availability of systems and data. Cyber threats can be classified according to the

targets directly affected. The source of a cyber threat is an entity that has the intention and carry out actions that violate the law and norms of information and asset security intending to obtain material or immaterial benefits through cyberspace (Aslan et al., 2023). The source of a cyber threat can come from within and outside, such as intelligence, disappointment, investigation, extremist organizations, hacktivists, organized crime groups, competition, hostility and conflict, and technology. Cyber threats include aspects of ideology, politics, economy, culture, defense, science and technology, and other things related to national and state life, including personal interests. Anyone, whether an individual or an organization, can be a source of cyber threats (Jacobsen, 2021).

Cyber threats such as infiltration and information leaks through communication protocols must be accepted with caution because if not controlled, they can turn into cyber attacks that can endanger information assets. A cyber attack is an act to enter, modify, steal, or damage an information system. Intense and large-scale cyber attacks can affect national defense. Therefore, in this study, the researcher views that cyber threats are a problem that must be addressed by involving parties such as non-state actors to protect critical infrastructure and maintain important data and information in Indonesia (Saxena et al., 2020).

C. METHOD

This research will be conducted using a qualitative approach. Through this approach, research data will be obtained from various good sources such as research results and previous studies that are still relevant to the content of the research. A qualitative approach allows for exploring and understanding complex and dynamic phenomena in the context of cybersecurity, especially in the implementation of machine learning for anomaly detection. When the research data has been successfully collected, the next step is to process the data systematically to find significant results. This analysis will help in outlining how machine learning can be implemented effectively in cybersecurity systems, as well as the challenges and opportunities it faces. Thus, the results of this study are expected to provide a significant contribution to the development of a more adaptive and responsive cybersecurity strategy to evolving threats (Nartin et al., 2024).

D. RESULT AND DISCUSSION

1. Challenges in Cyber Security Systems

In recent years, the cyber threat landscape has evolved dramatically, with attacks increasingly complex. Cybercriminals are now using a variety of sophisticated techniques to infiltrate and compromise security systems, including the use of highly stealthy malware, more convincing phishing attacks, and the exploitation of previously unknown zero-day vulnerabilities. The ability of attackers to rapidly adapt and modify their attack methods makes detection increasingly difficult. These increasingly complex attacks often leverage distributed botnets, artificial intelligence, and machine learning to outwit traditional security systems and bypass existing defenses. This presents a major challenge for security professionals who must always

stay ahead of attackers.

The limitations of traditional methods for detecting and preventing cyberattacks are also a major concern. Rule-based and signature-based security systems are generally only effective against known threats, as they work by matching known patterns to incoming data. These methods have significant weaknesses when it comes to new, unidentified attacks. As zero-day attacks and new malware variants designed to evade signature detection emerge, security systems that rely on traditional methods are becoming less effective. Additionally, manually adjusting rules for each new threat is a slow and inefficient process, often leading to delays in detection and response to attacks (Heidari & Jabraeil Jamali, 2023).

The volume and variability of data that must be analyzed in a cybersecurity context also presents a major challenge. Every day, organizations generate and must monitor large amounts of data from multiple sources such as network logs, user activity data, and system operational data. This data is not only large in volume but also highly variable in format and structure, making the analysis process extremely complex. Identifying suspicious patterns amidst a sea of unstructured and diverse data requires sophisticated analytical capabilities. The difficulty of managing and analyzing this data is further compounded by the fact that the data often has to be interpreted in a specific context, with each potential anomaly requiring careful assessment to avoid misidentification.

The need for real-time detection and response cannot be ignored in discussions about cybersecurity system challenges. When an attack is successful, every second that passes without detection can mean greater damage, data loss, and significant financial impact. Therefore, the ability to detect threats in real-time and respond quickly to them is critical to minimizing damage. However, achieving real-time detection is not an easy task. Systems must be able to quickly and accurately analyze incoming data, identify potential threats, and take corrective action within seconds. This requires robust computing infrastructure, efficient algorithms, and operational setups that can handle high workloads without sacrificing speed or accuracy.

The challenges in cybersecurity systems are diverse and complex. The increasing complexity of attacks, the limitations of traditional methods, the sheer volume and variability of data, and the need for real-time detection and response all require a more advanced and integrated approach. Future security systems must be more adaptive, powered by advanced technologies such as machine learning and artificial intelligence, to be able to address evolving threats and protect digital assets more effectively. The role of machine learning in this context becomes crucial, as it provides the ability to analyze data at scale and detect unexpected patterns, which is key to increasing resilience against increasingly sophisticated cyber threats.

2. The Role of Machine Learning in Anomaly Detection

Machine learning has opened a new chapter in cybersecurity, especially in anomaly detection. In this context, enhanced analytical capabilities are one of the main advantages of machine learning. Machine learning algorithms can analyze large amounts of data with high complexity much more effectively than traditional

methods. While rule-based and signature-based approaches require the explicit definition of threat patterns, machine learning models can identify anomalies based on behavioral patterns that are not immediately recognized as threats at first. These algorithms, such as deep learning and neural networks, can dig deeper into the data, extract relevant features, and identify complex correlations between seemingly unrelated variables. This allows for earlier and more accurate threat detection, allowing for faster and more targeted responses.

The ability of machine learning to detect unexpected patterns is a key factor in increasing the effectiveness of anomaly detection. Anomalies in the context of cybersecurity often do not follow patterns that are known or anticipated. Machine learning models, especially those using unsupervised learning techniques, can identify anomalies by observing deviations from existing normal patterns. For example, clustering models such as K-means or outlier detection algorithms can identify unusual activity based on the distribution of data they have learned. In other words, these models do not require prior knowledge of what constitutes a threat, but can dynamically learn from existing data to recognize abnormal behavior. This provides a significant advantage in the face of zero-day attacks and new and evolving attack methods (Quatrini et al., 2020).

Adapting to new attacks is also a significant advantage of machine learning in anomaly detection. The dynamic nature of cyber threats requires security systems to be constantly vigilant and able to adapt quickly. Machine learning models, especially those using reinforcement learning and online learning techniques, can continuously update themselves based on new incoming data. For example, intrusion detection models that use machine learning can be adjusted and improved in real-time based on new network traffic data. With this capability, the model can recognize new attack patterns and adjust its detection parameters to improve accuracy. This rapid and continuous adaptation is critical in the ever-changing cybersecurity environment, where new threats can emerge at any time and in many unexpected forms.

Reducing false positives and false negatives is a major focus in improving detection accuracy. False positives occur when a security system flags normal activity as a threat, while false negatives occur when a real threat is not detected. Machine learning can help reduce both types of errors through techniques such as supervised learning, where models are trained with labeled data to recognize the difference between normal and anomalous activity. With a comprehensive and representative dataset, models can learn to make more accurate decisions and reduce false alarms that can disrupt normal operations and drain resources. Additionally, ensemble learning methods that combine multiple machine learning models can improve detection accuracy by reducing variability and bias in predictions. This technique allows the system to produce more reliable and consistent results, increasing confidence in anomaly detection.

The role of machine learning in anomaly detection brings many significant benefits to cybersecurity. Enhanced analytical capabilities, detection of unexpected patterns, adaptation to new attacks, and reduction of false positives and negatives all contribute to creating a more robust and responsive security system. As machine

learning technologies and methods continue to advance, the future of anomaly detection in cybersecurity looks increasingly promising. Integrating machine learning into cybersecurity strategies not only helps in detecting and responding to threats more effectively but also enables organizations to stay one step ahead of attackers, protecting their data and digital assets from ever-evolving and increasingly sophisticated threats.

3. Implementation of Machine Learning in Cyber Security

Implementing machine learning in cybersecurity involves a series of complex and detailed steps to ensure the model can function effectively in detecting and responding to threats. The process of training a model begins with the collection of relevant data. Cybersecurity data often includes network logs, traffic data, user activity logs, and system operational data. The first step in model training is to clean and prepare this data, including handling missing values, data normalization, and feature transformation. Once the data is ready, the next step is to select and implement the right machine-learning algorithm. Algorithms such as deep learning, random forests, and support vector machines are often used in this context. The model is then trained with the prepared data, where the algorithm learns to recognize patterns and anomalies that indicate potential threats.

Relevant data sources are critical in training machine learning models for cybersecurity. Different types of data are needed to provide a complete picture of network activity and potential threats. Network logs are one of the primary data sources, recording every packet of data that passes through the network and providing detailed information about the origin, destination, and contents of the packet. Network traffic data, which includes communication patterns between devices, is also critical. Additionally, user activity logs that record user actions within the system, such as logins, file access, and configuration changes, can help detect unusual or suspicious behavior. System operational data, such as CPU and memory usage, can provide indications of abnormal activity that may be caused by malware or other attacks. By combining these multiple data sources, machine learning models can be trained to more accurately recognize different types of threats.

Integrating machine learning models with existing security systems is a crucial step to ensure effective threat detection and response. Machine learning models must be integrated into existing security infrastructure without disrupting normal operations. This process often involves setting up a data pipeline where relevant security data is continuously collected and processed by the machine learning model. This integration also requires tuning and calibrating the model to suit the specific characteristics and needs of the network or system being protected. Additionally, integration must ensure that the model's anomaly detection results can be communicated to security information management systems (SIEMs) and other monitoring tools to enable automated or manual responses to detected threats. With proper integration, machine learning models can strengthen existing layers of defense, providing more sophisticated detection and faster response to threats.

Model monitoring and updating is a critical aspect of implementing machine

learning for cybersecurity. Once a model is implemented, its performance must be continuously monitored to ensure its effectiveness in detecting new threats. The cyber threat landscape is highly dynamic, with new threats constantly emerging and attack techniques constantly evolving. Therefore, machine learning models must be regularly updated with new data and retrained to maintain their accuracy and relevance. This process involves continuously monitoring the model's performance using metrics such as accuracy, precision, recall, and F1-score. When model performance declines, it may be an indication that the model requires additional training data or parameter adjustments. Additionally, monitoring also helps identify potential biases or errors in the model, allowing for necessary adjustments to improve detection performance. With consistent monitoring and updating, machine learning models can continue to provide value in improving cybersecurity.

Implementing machine learning in cybersecurity is a comprehensive and ongoing process. From training the model with relevant data, and integrating the model into existing systems, to continuous monitoring and updating, each step requires careful attention and ongoing adjustments. Machine learning technology has great potential to detect and respond to cyber threats more effectively, but its success depends on proper implementation and ongoing maintenance. With a structured and comprehensive approach, machine learning can be a very powerful tool in the effort to protect information systems and data from increasingly complex and sophisticated cyber threats.

4. Evaluation and Measurement of Success

Evaluating and measuring the success of machine learning models in anomaly detection is a critical aspect of ensuring the effectiveness and reliability of cybersecurity systems. One of the primary methods for evaluating model performance is by using accuracy metrics. Accuracy measures the percentage of correct predictions out of the total predictions made by the model. Although accuracy is a commonly used metric, in the context of cybersecurity, it is often insufficient to fully describe the performance of a model, especially due to the imbalance of normal and anomalous activity in the data. Therefore, other metrics such as precision, recall, and F1-score are often used. Precision measures the percentage of correct anomaly detections out of all anomaly detections generated by the model, while recall measures the percentage of anomalies that are detected out of all anomalies. F1-score is a compromise between precision and recall, providing a more balanced picture of a model's performance in detecting anomalies. By using a combination of these metrics, we can gain a more comprehensive understanding of a model's ability to detect threats accurately and consistently.

The application of machine learning models in real-world scenarios often produces mixed results, depending on factors such as data quality, network complexity, and the nature of the threats encountered. Case studies of model implementation in operational environments provide valuable insights into the effectiveness of this approach. For example, in some cases, machine learning models have successfully identified anomalous patterns that were previously undetected by

traditional systems, allowing security teams to respond to threats faster and more appropriately. Furthermore, the implementation of models in real-world scenarios has also shown that machine learning models can adapt to changing network dynamics and threat patterns, providing more proactive protection. These successes reflect the great potential of machine learning in improving cybersecurity, although results may vary depending on the specific context and implementation strategy used.

However, evaluating machine learning models in dynamic operating environments presents its challenges. One major challenge is high data variability, where normal and anomalous patterns can change over time. These changes can be caused by factors such as increased traffic volume, changes in network configuration, or even unexpected legitimate user activity. Consistent and accurate evaluation under these conditions requires continuous monitoring and dynamic model adjustment. In addition, issues such as missing or incomplete data, mislabeling of training data, and bias in the data can also affect model performance. These challenges call for more sophisticated and adaptive evaluation approaches, including the use of cross-validation techniques and testing under diverse conditions to ensure that models remain reliable and effective across situations.

Looking to the future, recent advances in machine learning technology promise further improvements in anomaly detection. New techniques such as deep reinforcement learning and generative adversarial networks (GANs) offer the potential to enhance models' ability to recognize and respond to threats with greater sophistication. Deep reinforcement learning, for example, enables models to learn and adapt in rapidly changing environments through reinforcement and penalty mechanisms. Meanwhile, GANs can be used to generate realistic simulation data, helping to train models with more varied and complex threat scenarios. Furthermore, the integration of machine learning with other technologies such as blockchain and the Internet of Things (IoT) opens up new opportunities to create more decentralized and multi-layered security systems. With these advancements, the future of anomaly detection in cybersecurity looks increasingly promising, with the potential to provide stronger and more responsive protection against evolving threats.

Evaluating and measuring the success of machine learning models in cybersecurity requires a holistic and adaptive approach. By using the right metrics, studying the results of field implementations, addressing evaluation challenges in a dynamic environment, and leveraging the latest technological developments, we can continue to improve anomaly detection capabilities. Machine learning plays a critical role in the future of cybersecurity, providing more sophisticated and adaptive tools to protect information systems and data from increasingly complex and diverse threats.

E. CONCLUSION

Machine learning has become a critical pillar in the quest to improve cybersecurity, especially in anomaly detection. Enhanced analytical capabilities, detection of unexpected patterns, adaptation to new attacks, and reduction of false positives and negatives make machine learning a highly effective tool in detecting increasingly complex and diverse threats. The implementation process involves

careful steps ranging from training the model with relevant data, and integration into existing systems, to continuous monitoring and updating to maintain its reliability. Evaluation of the success of machine learning models in anomaly detection shows promising results in real-world scenarios, despite challenges such as data variability and changing dynamics of the operational environment. By using the right metrics and leveraging the latest technological developments, machine learning models continue to evolve to provide more effective and responsive protection against cyber threats. The future of anomaly detection in cybersecurity looks bright, with machine learning expected to play an increasingly large role in protecting systems and data from evolving threats.

REFERENCES

1. Akalin, N., & Loutfi, A. (2021). Reinforcement learning approaches in social robotics. Sensors, 21(4), 1292.
2. Al-amri, R., Murugesan, R. K., Man, M., Abdulateef, A. F., Al-Sharafi, M. A., & Alkahtani, A. A. (2021). A review of machine learning and deep learning techniques for anomaly detection in IoT data. Applied Sciences, 11(12), 5320.
3. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.
4. Balaji, T. K., Annavarapu, C. S. R., & Bablani, A. (2021). Machine learning algorithms for social media analysis: A survey. Computer Science Review, 40, 100395.
5. Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in industry, 114, 103165.
6. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.
7. Dong, S. (2021). Multi class SVM algorithm with active learning for network traffic classification. Expert Systems with Applications, 176, 114885.
8. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. Cluster Computing, 26(6), 3753-3780.
9. Jacobsen, J. T. (2021). Cyber offense in NATO: challenges and opportunities. International affairs, 97(3), 703-720.
10. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.
11. Klenka, M. (2021). Aviation cyber security: legal aspects of cyber threats. Journal of transportation security, 14(3), 177-195.
12. Nartin, S. E., Faturrahman, S. E., Ak, M., Deni, H. A., MM, C., Santoso, Y. H., ... & Eliyah, S. K. (2024). Metode penelitian kualitatif. Cendikia Mulia Mandiri.
13. Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., &

Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, 102494.
14. Omuya, E. O., Okeyo, G. O., & Kimwele, M. W. (2021). Feature selection for classification using principal component analysis and information gain. Expert Systems with Applications, 174, 114765.
15. Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1), 103-128.
16. Quatrini, E., Costantino, F., Di Gravio, G., & Patriarca, R. (2020). Machine learning for anomaly detection and process phase classification to improve safety and maintenance activities. Journal of Manufacturing Systems, 56, 117-132.
17. Rahmani, A. M., Yousefpoor, E., Yousefpoor, M. S., Mehmood, Z., Haider, A., Hosseinzadeh, M., & Ali Naqvi, R. (2021). Machine learning (ML) in medicine: Review, applications, and challenges. Mathematics, 9(22), 2970.
18. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. Electronics, 9(9), 1460.
19. Smith, R., Friston, K. J., & Whyte, C. J. (2022). A step-by-step tutorial on active inference and its application to empirical data. Journal of mathematical psychology, 107, 102632.
20. Sturgeon, T. J. (2021). Upgrading strategies for the digital economy. Global strategy journal, 11(1), 34-57.
21. Sujith, A. V. L. N., Qureshi, N. I., Dornadula, V. H. R., Rath, A., Prakash, K. B., & Singh, S. K. (2022). A comparative analysis of business machine learning in making effective financial decisions using structural equation model (SEM). Journal of Food Quality, 2022(1), 6382839.
22. Taye, M. M. (2023). Understanding of machine learning with deep learning: architectures, workflow, applications and future directions. Computers, 12(5), 91.
23. Trim, P. R., & Lee, Y. I. (2021). The global cyber security model: counteracting cyber attacks through a resilient partnership arrangement. Big Data and Cognitive Computing, 5(3), 32.
24. Turk, Ž., de Soto, B. G., Mantha, B. R., Maciel, A., & Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. Automation in Construction, 133, 103988.
25. Vercio, L. L., Amador, K., Bannister, J. J., Crites, S., Gutierrez, A., MacDonald, M. E., ... & Forkert, N. D. (2020). Supervised machine learning tools: a tutorial for clinicians. Journal of Neural Engineering, 17(6), 062001.