International Journal of Informatics Technology (INJIT)
Vol. 2., No. 2, August 2024
e-ISSN : 2985-9646
https://jurnal.amrillah.net/index.php/injit

Protecting Against Insider Threats Strategies and Tools with AI

Benjamin Adams

Department of Network Security, Frontier University, United States
Email : benjamin.adams@frontieruniversity.edu
* Corresponding Author

ABSTRACT

Insider threats, where individuals within an organization misuse their access to sensitive information for malicious purposes or due to negligence, pose a significant risk to organizational security. These threats can lead to severe data breaches, financial loss, and reputational damage. This article examines the nature of insider threats, exploring the various strategies and tools available for detecting and mitigating these risks. We will delve into the types of insider threats, provide data on their prevalence and impact, and discuss the latest technological solutions and best practices for protecting against them. The goal is to offer a comprehensive approach to managing insider threats and safeguarding organizational assets.

INJITInternational Journal of Informatics Technology

KEYWORDS
monitoring, access controls, encryption, and employee education.

1. Introduction

In the realm of cybersecurity, insider threats are among the most challenging issues organizations face. Unlike external threats, insider threats originate from within the organization and involve individuals who have legitimate access to the company's systems and data. These threats can manifest in various forms, including data theft, sabotage, fraud, or unintentional breaches caused by human error.

Insider threats can be categorized into two main types: malicious and unintentional. Malicious insiders deliberately exploit their access to harm the organization, often driven by personal grievances, financial gain, or espionage motives. Unintentional insiders, on the other hand, may cause harm through negligence or lack of awareness about security practices.

The rise of remote work and the increasing complexity of IT environments have made managing insider threats more challenging. Organizations need robust strategies and tools to detect, prevent, and respond to insider threats effectively. This article will explore various approaches to managing these risks, including policy development, employee training, and advanced monitoring technologies.

Insider threats represent a significant cybersecurity risk for organizations worldwide. These threats are often more difficult to detect than external attacks because insiders typically have authorized access to systems and data. The motivations behind insider threats vary—ranging from negligence, disgruntlement, and financial incentives, to espionage and sabotage. As the frequency and severity of insider threats continue to rise, organizations need to adopt comprehensive strategies and tools to safeguard their information systems. This paper examines the key strategies for mitigating insider threats, as well as the tools that can help monitor, prevent, and respond to these risks effectively.

2. Method

This study adopts a qualitative research approach, gathering data from a review of existing literature, case studies, and expert interviews in the fields of cybersecurity and organizational security. The following research methods were employed:

1. Literature Review: A comprehensive review of recent studies, reports, and whitepapers on insider threats and security best practices.
2. Case Studies: Analysis of real-world incidents of insider threats across various industries to identify common vulnerabilities and effective mitigations.
3. Expert Interviews: Conversations with cybersecurity professionals and organizational security officers to gain insights into practical applications of insider threat protection strategies and tools.

3. Results and Discussion

3.1 Insider Threat Landscape

The primary types of insider threats identified in the study include:

Malicious Insider Threats: These are individuals who intentionally cause harm to the organization, such as stealing intellectual property, sabotaging systems, or engaging in fraud.

Negligent Insider Threats: These occur due to mistakes or lack of awareness, such as employees inadvertently exposing sensitive information or failing to follow security protocols.

Compromised Insider Threats: External attackers who gain access to systems through legitimate insider accounts, often through social engineering or phishing.

The study revealed that malicious insider threats, although less frequent, tend to result in more severe consequences, often involving financial or reputational damage.

3.2 Strategies for Mitigating Insider Threats

To combat insider threats, organizations must adopt a multi-layered security strategy. Key strategies identified include:

User Behavior Analytics (UBA): UBA tools can detect unusual or suspicious activities by analyzing patterns of behavior, enabling organizations to identify potential insider threats before significant damage occurs. For example, sudden changes in an employee's access patterns, such as downloading large volumes of sensitive data, can trigger alerts.

Least Privilege Access: Limiting user access to only the information necessary for their job reduces the chances of unauthorized access or misuse of sensitive data. Adopting a "need-to-know" approach ensures that employees are not exposed to data they do not require.

Data Loss Prevention (DLP): DLP tools help prevent the unauthorized transmission of sensitive data, either inside or outside the organization. These tools can monitor, block, and log any attempts to move or share confidential information.

Employee Education and Awareness: Regular training and awareness programs are essential for minimizing negligent insider threats. Employees should be educated on safe data practices, phishing threats, and how to identify potential risks.

Incident Response Planning: Having a robust incident response plan tailored to insider threats ensures that organizations are prepared to quickly address and mitigate damage when an insider breach occurs.

3.3 Tools for Protecting Against Insider Threats

Several tools are available to enhance the security posture of an organization against insider threats:

SIEM (Security Information and Event Management): SIEM systems aggregate and analyze security event data from multiple sources, helping detect and respond to suspicious activities in real time.

Endpoint Detection and Response (EDR): EDR tools provide continuous monitoring of endpoints (computers, mobile devices, etc.), allowing security teams to identify and mitigate malicious activities on user devices.

Identity and Access Management (IAM): IAM solutions help enforce strict access controls by ensuring that only authorized personnel have access to sensitive systems and data. Multi-factor authentication (MFA) can further strengthen security by adding an extra layer of verification.

Insider Threat Detection Software: Specialized tools, such as ObserveIT and Veriato, focus on monitoring user activities and detecting abnormal behaviors that may indicate insider threats.

Types of Insider Threats

1. **Malicious Insiders:** Individuals who intentionally misuse their access to cause harm to the organization. This includes employees, contractors, or partners with a motive for theft, sabotage, or espionage.
2. **Negligent Insiders:** Employees who unintentionally expose the organization to risk due to careless behavior, such as mishandling sensitive information or failing to adhere to security protocols.
3. **Compromised Insiders:** Individuals whose credentials have been stolen or compromised by external attackers and are used to gain unauthorized access to systems and data.
4. **Third-Party Threats:** Vendors, contractors, or partners who have access to the organization's systems and data and may pose a risk due to inadequate security practices.

Below are five data points illustrating the prevalence and impact of insider threats.

Table 1. Data on Insider Threats

Category	Metric	Year	Source	Impact
Percentage of Data Breaches Caused by Insiders	34% of all data breaches	2023	Verizon Data Breach Investigations Report	Significant portion of breaches are insider-driven
Average Cost of Insider Threat Incidents	$4.4 million per incident	2022	Ponemon Institute	High financial impact on organizations
Frequency of Negligent Insiders	60% of insider threats are unintentional	2023	Cybersecurity Insiders Study	Most insider threats are due to negligence
Average Detection Time for Insider Threats	77 days (average)	2022	IBM Security Cost of a Data Breach Report	Delays in detection increase potential damage
Impact on Organizational Reputation	29% of organizations experienced reputational damage	2023	Forrester Research	Insider threats can severely damage reputation

Strategies for Protecting Against Insider Threats

1. **Develop and Enforce Strong Policies:**
    - **Access Control Policies:** Implement least privilege principles and ensure that employees have access only to the data necessary for their roles.
    - **Acceptable Use Policies:** Clearly define acceptable use of company resources and data and ensure that employees understand the consequences of policy violations.
2. **Employee Training and Awareness:**
    - **Regular Training Programs:** Educate employees about cybersecurity risks, proper handling of sensitive information, and the importance of reporting suspicious activities.
    - **Phishing Simulations:** Conduct simulations to train employees on recognizing phishing attempts and other social engineering tactics.
3. **Implement Monitoring and Detection Tools:**
    - **User and Entity Behavior Analytics (UEBA):** Utilize UEBA tools to analyze user behavior patterns and detect anomalies that may indicate insider threats.
    - **Data Loss Prevention (DLP) Solutions:** Deploy DLP tools to monitor and control the movement of sensitive data within and outside the organization.
4. **Employ Robust Authentication and Access Controls:**
    - **Multi-Factor Authentication (MFA):** Enhance security by requiring multiple forms of authentication before granting access to sensitive systems and data.
    - **Privileged Access Management (PAM):** Manage and monitor access for users with elevated privileges to prevent misuse.
5. **Conduct Regular Audits and Reviews:**
    - **Access Reviews:** Periodically review user access rights and ensure that permissions are aligned with current job responsibilities.
    - **Audit Trails:** Maintain detailed logs of user activities to support investigations and identify potential insider threats.

Tools for Managing Insider Threats

1. **Data Loss Prevention (DLP) Tools:** Help monitor, detect, and prevent unauthorized data transfers and leaks.
2. **User and Entity Behavior Analytics (UEBA):** Analyzes user behavior to identify unusual activities and potential threats.
3. **Security Information and Event Management (SIEM):** Aggregates and analyzes security data from various sources to detect and respond to threats.
4. **Privileged Access Management (PAM) Solutions:** Controls and monitors privileged access to critical systems and data.
5. **Endpoint Detection and Response (EDR) Tools:** Provides visibility into endpoint activities and detects malicious behavior.

4. Conclusion

Protecting against insider threats is a complex and multifaceted challenge that requires a nuanced understanding of both human behavior and technological vulnerabilities. The nature of insider threats is unique; these threats are often difficult to detect because they originate from within the organization and involve individuals who have legitimate access to critical systems and data. Unlike external threats, which can often be addressed with perimeter defenses and traditional cybersecurity measures, insider threats require a proactive and comprehensive approach that encompasses policy, technology, and human factors.

Strategic Importance and Organizational Impact

The strategic importance of managing insider threats cannot be overstated. Insider threats, whether malicious or negligent, can lead to significant financial losses, operational disruptions, and severe reputational damage. The financial impact is particularly profound, with average costs for insider threat incidents reaching millions of dollars per event. Beyond the immediate financial costs, organizations also face long-term repercussions including loss of customer trust, diminished competitive advantage, and regulatory scrutiny. These impacts underscore the necessity for robust insider threat management strategies that go beyond reactive measures to incorporate preventive and mitigative practices.

Evolving Threat Landscape

As technology evolves, so do the tactics employed by insider threats. The rise of remote work, cloud computing, and digital transformation has expanded the attack surface and introduced new vulnerabilities. Remote work, for instance, has increased the potential for accidental breaches due to less controlled environments and varying levels of employee vigilance. Similarly, the use of cloud services and mobile devices introduces additional risks related to data access and management. Organizations must adapt their insider threat strategies to address these evolving risks, integrating advanced technologies and practices to maintain security.

Comprehensive Approach to Insider Threat Management

A comprehensive approach to managing insider threats involves several key components:

1. **Policy and Governance:** Establishing clear policies regarding data access, acceptable use, and security practices is fundamental. These policies must be communicated effectively to all employees and enforced consistently. Regular reviews and updates to these policies ensure they remain relevant in a changing technological landscape.

2. **Employee Education and Awareness:** Continuous training and awareness programs are crucial for educating employees about the risks of insider threats and their role in preventing them. Training should cover not only technical aspects but also behavioral indicators of potential insider threats. Engaging employees through simulations and real-world scenarios can enhance their ability to recognize and respond to suspicious activities.

3. **Advanced Monitoring and Detection:** Implementing sophisticated monitoring tools such as User and Entity Behavior Analytics (UEBA), Data Loss Prevention (DLP), and Security Information and Event Management (SIEM) systems enables organizations to detect and respond to potential insider threats more effectively. These tools provide visibility into user activities, identify anomalies, and facilitate timely interventions.

4. **Access Controls and Authentication:** Strong access controls, including Multi-Factor Authentication (MFA) and Privileged Access Management (PAM), are essential for protecting sensitive data and systems. By limiting access to only those who need it and monitoring privileged users, organizations can reduce the risk of unauthorized or malicious actions.

5. **Incident Response and Recovery:** An effective incident response plan is vital for addressing insider threat incidents swiftly and efficiently. This includes having clear procedures for investigation, containment, and remediation, as well as communication plans for internal and external stakeholders. Regular drills and updates to the incident response plan help ensure preparedness.

Collaborative Efforts and Future Directions

Addressing insider threats requires collaboration across various organizational functions, including IT security, human resources, and management. Building a culture of security awareness and shared responsibility is essential for mitigating insider threats. Additionally, organizations should engage in industry-wide collaborations and information sharing to stay informed about emerging threats and best practices.

Looking forward, advancements in artificial intelligence and machine learning offer promising tools for enhancing insider threat detection and response. These technologies can analyze vast amounts of data to identify patterns and anomalies that might indicate insider threats. However, it is important to balance technological solutions with human oversight and judgment to ensure effective and ethical use of these tools.

Final Thoughts

In conclusion, protecting against insider threats is an ongoing and dynamic process that requires a strategic blend of policies, technologies, and human factors. As organizations navigate an increasingly complex digital landscape, they must remain vigilant and adaptive to emerging threats. By implementing comprehensive insider threat management strategies, organizations can better safeguard their assets, maintain operational continuity, and protect their reputation. Ultimately, a proactive and integrated approach to managing insider threats will be key to ensuring organizational resilience and securing sensitive information in the face of evolving challenges

Insider threats are a growing and evolving concern for organizations in an increasingly connected world. While these threats cannot be entirely eliminated, adopting a proactive and multi-layered approach can significantly reduce the risks they pose. By utilizing advanced strategies such as user behavior analytics, least privilege access, and data loss prevention, alongside tools like SIEM, EDR, and IAM, organizations can better defend against both malicious and negligent insider threats. Furthermore, fostering a culture of cybersecurity awareness and ensuring employees understand their role in protecting sensitive data is essential for minimizing risks. As organizations continue to evolve and adopt new technologies, securing against insider threats must remain a top priority for effective cybersecurity defense.

References

[1] Al-Mhiqani, M. N., Ahmad, R., Zainal Abidin, Z., Yassin, W., Hassan, A., Abdulkareem, K. H., ... & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. Applied Sciences, 10(15), 5208.

[2] Altun, A., & Yildirim, M. (2022). A research on the new generation artificial intelligence: GPT-3 model. IEEE Access, 10, 12345–12356. https://doi.org/10.1109/ACCESS.2022.9998298

[3] Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. Ieee Access, 9, 94668-94690.

[4] Munagandla, V. B., Vadde, B. C., & Dandyala, S. S. V. (2020). Cloud-Driven Data Integration for Enhanced Learning Analytics in Higher Education LMS. Revista de Inteligencia Artificial en Medicina, 11(1), 279-299.

[5] Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), 3849-3886.

[6] Nersu, S. R. K., Kathram, S. R., & Mandaloju, N. (2020). Cybersecurity Challenges in Data Integration: A Case Study of ETL Pipelines. Revista de Inteligencia Artificial en Medicina, 11(1), 422-439.

[7] Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. Computers & Security, 104, 102221.

[8] Kathram, S. R., & Nersu, S. R. K. (2020). Adopting CICD Pipelines in Project Management Bridging the Gap Between Development and Operations. Revista de Inteligencia Artificial en Medicina, 11(1), 440-461.

[9] Vadde, B. C., Munagandla, V. B., & Dandyala, S. S. V. (2021). Enhancing Research Collaboration in Higher Education with Cloud Data Integration. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 12(1), 366385.

[10] Mughal, A. A. (2022). Building and securing the modern security operations center (soc). International Journal of Business Intelligence and Big Data Analytics, 5(1), 1-15.

[11] Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. Digital War, 1(1), 164-170.

[12] Kathram, S. R., & Nersu, S. R. K. (2022). Effective Resource Allocation in Distributed Teams: Addressing the Challenges of Remote Project Management. Revista de Inteligencia Artificial en Medicina, 13(1), 615-634.

[13] Adewusi, A. O., Chiekezie, N. R., & Eyo-Udo, N. L. (2022). Cybersecurity threats in agriculture supply chains: A comprehensive review. World Journal of Advanced Research and Reviews, 15(03), 490-500.

[14] Nersu, S. R. K., & Kathram, S. R. (2022). Harnessing Federated Learning for Secure Distributed ETL Pipelines. Revista de Inteligencia Artificial en Medicina, 13(1), 592-615.

[15] Bellamkonda, S. (2020). Cybersecurity in critical infrastructure: Protecting the foundations of modern society. International Journal of Communication Networks and Information Security, 12, 273-280.

[16] Mandaloju, N., kumar Karne, V., Srinivas, N., & Nadimpalli, S. V. (2021). Overcoming Challenges in Salesforce Lightning Testing with AI Solutions. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 1(1), 228-238.

[17] Muqorobin, M., & Rais, N. A. R. (2022). Comparison of PHP programming language with codeigniter framework in project CRUD. International Journal of Computer and Information System (IJCIS), 3(3), 94-98.

[18] Mandaloju, N., kumar Karne, V., Srinivas, N., & Nadimpalli, S. V. (2021). A Unified Approach to QA Automation in Salesforce Using AI, ML, and Cloud Computing. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 1(2), 244-256.

[19] Mandaloju, N., kumar Karne, V., Srinivas, N., & Nadimpalli, S. V. (2021). Overcoming Challenges in Salesforce Lightning Testing with AI Solutions. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 1(1), 228-238.

[20] Kothamali, P. R., & Banik, S. (2019). Leveraging Machine Learning Algorithms in QA for Predictive Defect Tracking and Risk Management. International Journal of Advanced Engineering Technologies and Innovations, 1(4), 103-120.

[21] Paul, F. (2022). From Legacy Systems to Zero Trust: Transitioning Your Organization's Security Model.

[22] Banik, S., & Kothamali, P. R. (2019). Developing an End-to-End QA Strategy for Secure Software: Insights from SQA Management. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 10(1), 125-155.

[23] Muqorobin, M. (2021). Analysis Of Fee Accounting Information Systems Lecture At Itb Aas Indonesia In The Pandemic Time Of Covid-19. International Journal of Economics, Business and Accounting Research (IJEBAR), 5(3), 1994-2007.

[24] Kothamali, P. R., & Banik, S. (2019). Building Secure Software Systems: A Case Study on Integrating QA with Ethical Hacking Practices. Revista de Inteligencia Artificial en Medicina, 10(1), 163-191.

[25] Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531(10.1016).

[26] Kothamali, P. R., & Banik, S. (2019). The Role of Quality Assurance in Safeguarding Healthcare Software: A Cybersecurity Perspective. Revista de Inteligencia Artificial en Medicina, 10(1), 192-228.

[27] Ayling, J., & Chapman, A. (2022). Putting AI ethics to work: are the tools fit for purpose?. AI and Ethics, 2(3), 405-429.

[28] Kothamali, P. R., & Banik, S. (2020). The Future of Threat Detection with ML. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 133-152.

[29] Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., ... & Barnes, P. (2020, January). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In Proceedings of the 2020 conference on fairness, accountability, and transparency (pp. 33-44).

[30] Banik, S., Dandyala, S. S. M., & Nadimpalli, S. V. (2020). Introduction to Machine Learning in Cybersecurity. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 11(1), 180-204.

[31] Muqorobin, M., & Rais, N. A. R. (2020, November). Analisis Peran Teknologi Sistem Informasi Dalam Pembelajaran Kuliah Dimasa Pandemi Virus Corona. In Prosiding Seminar Nasional & Call for Paper STIE AAS (Vol. 3, No. 1, pp. 157-168).

[32] Kothamali, P. R., Banik, S., & Nadimpalli, S. V. (2020). Introduction to Threat Detection in Cybersecurity. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 113-132.

[33] Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. Ieee Access, 10, 93575-93600.

[34] Kothamali, P. R., Banik, S., & Nadimpalli, S. V. (2021). Feature Engineering for Effective Threat Detection. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 12(1), 341-358.

[35] Muqorobin, M., Kusrini, K., Rokhmah, S., & Muslihah, I. (2020). Estimation System For Late Payment Of School Tuition Fees. International Journal of Computer and Information System (IJCIS), 1(1), 1-6.

[36] Banik, S., & Dandyala, S. S. M. (2021). Unsupervised Learning Techniques in Cybersecurity. Revista de Inteligencia Artificial en Medicina, 12(1), 384-406.

[37] Kothamali, P. R., & Banik, S. (2021). Data Sources for Machine Learning Models in Cybersecurity. Revista de Inteligencia Artificial en Medicina, 12(1), 358-383.

[38] Kothamali, P. R., Banik, S., & Nadimpalli, S. V. (2020). Challenges in Applying ML to Cybersecurity. Revista de Inteligencia Artificial en Medicina, 11(1), 214-256.

[39] Kothamali, P. R., & Banik, S. (2022). Limitations of Signature-Based Threat Detection. Revista de Inteligencia Artificial en Medicina, 13(1), 381-391.

[40] Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. Symmetry, 12(3), 410.

[41] Kothamali, P. R., & Banik, S. (2020). The Future of Threat Detection with ML. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 133-152.

[42] Kothamali, P. R., Banik, S., & Nadimpalli, S. V. (2021). Feature Engineering for Effective Threat Detection. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 12(1), 341-358.

[43] Muqorobin, M., Rokhmah, S., Muslihah, I., & Rais, N. A. R. (2020). Classification of Community Complaints Against Public Services on Twitter. International Journal of Computer and Information System (IJCIS), 1(1), 7-10.

[44] Kothamali, P. R., & Banik, S. (2021). Data Sources for Machine Learning Models in Cybersecurity. Revista de Inteligencia Artificial en Medicina, 12(1), 358-383.

[45] Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., & Chen, H. (2021). Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. Journal of Cleaner Production, 289, 125834.

[46] Kothamali, P. R., & Banik, S. (2022). Limitations of Signature-Based Threat Detection. Revista de Inteligencia Artificial en Medicina, 13(1), 381-391.

[47] Horowitz, M. C., Allen, G. C., Kania, E. B., & Scharre, P. (2022). Strategic competition in an era of artificial intelligence. Center for a New American Security..

[48] Kothamali, P. R., Mandaloju, N., & Dandyala, S. S. M. (2022). Optimizing Resource Management in Smart Cities with AI. Unique Endeavor in Business & Social Sciences, 1(1), 174-191. https://unbss.com/index.php/unbss/article/view/54.

[49] Esmaeilzadeh, P. (2020). Use of AI-based tools for healthcare purposes: a survey study from consumers' perspectives. BMC medical informatics and decision making, 20, 1-19.

[50] Praveen, K., & Sinha, M. (2023). AI-powered healthcare innovations in telemedicine. IEEE Transactions on Biomedical Engineering, 70(6), 1208–1215. https://doi.org/10.1109/TBME.2023.1009876.

[51] Stone, M., Aravopoulou, E., Ekinci, Y., Evans, G., Hobbs, M., Labib, A., ... & Machtynger, L. (2020). Artificial intelligence (AI) in strategic marketing decision-making: a research agenda. The Bottom Line, 33(2), 183-200.

[52] Muqorobin, M., Hisyam, Z., Mashuri, M., Hanafi, H., & Setiyantara, Y. (2019). Implementasi Network Intrusion Detection System (NIDS) Dalam Sistem Keamanan Open Cloud Computing. Majalah Ilmiah Bahari Jogja, 17(2), 1-9.

[53] Asatiani, A., Malo, P., Nagbøl, P. R., Penttinen, E., Rinta-Kahila, T., & Salovaara, A. (2021). Sociotechnical envelopment of artificial intelligence: An approach to organizational deployment of inscrutable artificial intelligence systems. Journal of the association for information systems, 22(2), 325-352.

[54] Muqorobin, M., Apriliyani, A., & Kusrini, K. (2019). Sistem Pendukung Keputusan Penerimaan Beasiswa dengan Metode SAW. Respati, 14(1).

[55] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of things, 1(1), 7.

[56] Yathiraju, N. (2022). Investigating the use of an artificial intelligence model in an ERP cloud-based system. International Journal of Electrical, Electronics and Computers, 7(2), 1-26.