Journal of Computer Science and Technology Application (CORISINTA)
Vol. 1, No. 2, 2024, pp. 136∼143
E-ISSN:XXXX-XXXX P-ISSN: 3046-7616, DOI:XXX

Advanced Cyber Threat Detection: Big Data-Driven AI Solutions in Complex Networks

Agung Rizky[1*], Muhammad Zaki Firli[2], Nur Aulia Lindzani[3], Sipah Audiah[4], Lukita Pasha[5]
[1]Faculty of Digital Bussines, University of Raharja, Indonesia
[2]Faculty of Computer System, University of Raharja, Indonesia
[3,4,5]Faculty of Digital Business, CAI Sejahtera Indonesia, Indonesia
[1]agung.rizky@raharja.info, [2]m.zaki@raharja.info, [3]nur.aulia@raharja.info,
[4]sipah@raharja.info, [5]lukita@raharja.info
***Corresponding Author**

Article Info

Article history:

Received July 01, 2024
Revised August 13, 2024
Accepted Agusut 21, 2024

Keywords:

Cybersecurity
Artificial Intelligence
Big Data Analytics
Threat Detection
Network Security

ABSTRACT

In the rapidly evolving digital landscape, cybersecurity has become increasingly critical, especially within complex network environments. This research presents the development of a cyber threat detection system that leverages Artificial Intelligence (AI) and Big Data analytics to enhance accuracy and speed in identifying and responding to cyber threats. The system was evaluated through rigorous testing, demonstrating a high detection accuracy of 95% for malware and unauthorized access attempts, along with an impressive detection speed of 2 seconds on average for most threats. Additionally, the system exhibited strong scalability, maintaining optimal performance even with increasing network complexity. These findings underscore the system's robustness and practical applicability in real-world scenarios. However, further refinement is suggested to improve anomaly detection and reduce response times for more complex threats. This study contributes valuable insights into the integration of AI and Big Data in cybersecurity, providing a scalable and effective solution for protecting critical network infrastructures.

Corresponding Author:

Agung Rizky
Faculty of Digital Bussines, University of Raharja, Indonesia
agung.rizky@raharja.info

1. INTRODUCTION

In the rapidly evolving digital era, cybersecurity has become one of the most crucial aspects for individuals, organizations, and nations [1, 2]. The advancement of technology has driven increased connectivity and integration between various systems and networks, creating an increasingly complex network ecosystem [3–5]. These complex networks encompass various devices, from computers to Internet of Things (IoT) devices, connected through a vast and diverse network infrastructure [6]. As a result, these networks have become more vulnerable to various cyber threats, such as malware attacks, ransomware, denial-of-service (DoS) attacks, and data breaches.

The importance of cybersecurity in complex networks cannot be underestimated [7]. Cyber threats not only lead to financial losses but also cause reputational damage, operational disruptions, and privacy violations [8–11]. At the national level, cyber-attacks can threaten national security, damage critical infrastructure, and affect economic stability [12]. Therefore, implementing effective and innovative cybersecurity measures is

essential to protect the integrity, confidentiality, and availability of data and network systems [13].

Detecting cyber threats in modern networks presents significant challenges due to the vast volume of data generated by these complex systems. Each device connected to the network produces data that must be monitored and analyzed to detect suspicious patterns or anomalies that may indicate cyber threats [14]. Managing and analyzing this big data requires significant resources and sophisticated analytical techniques. Additionally, the constantly evolving nature of cyber threats complicates threat detection further [15]. Cyber attackers continuously develop new methods to exploit network vulnerabilities and evade detection, utilizing advanced techniques such as AI-based attacks, polymorphic attacks, and zero-day attacks [16–18].

Traditional security systems often rely on predefined rules and signatures, making them less effective in detecting new and unknown threats [16, 19, 20]. Furthermore, the diversity of devices and technologies connected to the network adds complexity in maintaining consistent and effective security across the entire network. This research aims to address these challenges by proposing an advanced cyber threat detection solution based on AI and Big Data analytics [21]. The primary objective is to develop a threat detection system that can quickly and accurately identify and respond to cyber threats in complex networks. The proposed system leverages the power of AI to recognize patterns and anomalies that cannot be detected by traditional systems and utilizes Big Data analytics to efficiently manage and analyze large volumes of data [22, 23].

1.1. Literature Review

The literature surrounding the integration of Artificial Intelligence (AI) and Big Data analytics in cybersecurity is extensive and highlights the significant advancements and challenges in the field. This section reviews key studies that have contributed to the understanding and development of AI-driven cybersecurity solutions, particularly in the context of complex networks [24].

1.1.1. AI in Cybersecurity

Artificial Intelligence (AI) has emerged as a transformative technology in the field of cybersecurity, offering more sophisticated and adaptive threat detection capabilities than traditional methods [25]. AI techniques, such as machine learning and deep learning, have shown remarkable success in identifying patterns and anomalies within large datasets, which are often indicative of potential cyber threats. Buczak and Guven (2016) demonstrated that machine learning algorithms could detect network anomalies more accurately by continuously learning from new data inputs [26]. This adaptability is critical in cybersecurity, where the nature of threats is constantly evolving.

Deep learning, a subset of AI, has proven particularly effective in analyzing unstructured data, such as network traffic logs and malware samples [27]. Deep learning models, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), can detect complex attack patterns in real-time, providing a significant improvement over traditional signature-based detection systems. These models can automatically extract features from raw data, enabling the detection of previously unknown threats with high accuracy.

1.1.2. Big Data Analytics in Cyber Threat Detection

Big Data analytics plays a pivotal role in enhancing cybersecurity, particularly in complex network environments where vast amounts of data are generated continuously. The ability to process and analyze this data efficiently is crucial for detecting and mitigating cyber threats [28]. One of the key contributions of Big Data analytics is its capacity for real-time data processing, which allows for the continuous monitoring and analysis of network traffic [29]. This real-time capability enables the detection of emerging threats, preventing cyber-attacks from causing significant damage before they can be mitigated. By leveraging real-time data, security systems can identify and respond to threats much faster than traditional methods that often rely on delayed batch processing. Additionally, Big Data analytics supports comprehensive threat detection by enabling the collection and analysis of extensive datasets from various sources, such as network logs, traffic data, and IoT devices [30]. This comprehensive approach allows for the identification of complex and hidden threats that may not be apparent through smaller-scale data analysis [31]. Techniques like clustering and classification can be applied to these large datasets to detect patterns and anomalies that indicate potential security breaches. For example, clustering can group similar data points together, revealing outliers that could signify a cyber threat [32].

1.1.3. Enhanced AI Model Training

Big Data analytics significantly enhances the effectiveness of AI models used in cyber threat detection by providing large and diverse datasets for training [33]. With access to extensive datasets, AI models can learn from a wider range of examples, improving their ability to detect both known threats and previously unseen vulnerabilities. This comprehensive training process ensures that AI-driven security systems are better equipped to identify complex attack patterns and respond to emerging cyber threats with greater accuracy. As a result, the integration of Big Data in AI model training leads to more robust and reliable threat detection capabilities [34].

2. THE COMPREHENSIVE THEORETICAL BASIS

This section outlines the methodology employed in developing and testing the advanced cyber threat detection system proposed in this research. The methodology is structured to provide a clear understanding of the system architecture, data collection and preprocessing, and the AI and Big Data techniques applied [35].

2.1. System Architecture

The proposed threat detection system is designed to leverage the combined power of Artificial Intelligence (AI) and Big Data analytics to detect and respond to cyber threats in complex networks [36]. The system architecture consists of four main components:

- Data Collection Module: Data is continuously collected from various sources, including network logs, traffic data, and IoT devices. The module is designed to handle large volumes of data and ensure seamless data flow into the system [37] .
- Data Preprocessing Module: Collected data undergoes preprocessing to remove noise and fill in missing values. This step ensures that the data used for analysis is clean and of high quality, which is crucial for accurate threat detection.
- AI-Based Analysis Module: The preprocessed data is analyzed using AI models that have been trained on extensive datasets. These models are capable of detecting suspicious patterns and anomalies that indicate potential cyber threats. The AI models employed include Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Random Forest algorithms.
- Threat Response Module: Upon detecting a threat, this module initiates predefined actions such as blocking suspicious traffic or alerting the security team. The response actions are designed to be both automated and rapid, minimizing the potential impact of detected threats

2.2. Data Collection and Preprocessing

Data for this system is collected from a variety of sources, including network logs, traffic data, and IoT devices. The data collection process is designed to operate in real-time, ensuring that the system has access to the most up-to-date information [38]. The data preprocessing involves several critical steps:

- Data Cleaning: Erroneous or inconsistent data is removed or corrected to ensure that only high-quality data is used in the analysis process.
- Data Normalization: Data is transformed into a consistent format to facilitate analysis. This step is particularly important in a complex network environment where data may be generated in various formats.
- Missing Value Imputation: Statistical or machine learning techniques are used to fill in missing values in the dataset, ensuring that the analysis is not compromised by incomplete data.

2.3. AI and Big Data Techniques

The effectiveness of the proposed threat detection system is largely driven by the integration of advanced AI and Big Data techniques [39]. The system employs a variety of machine learning and deep learning algorithms, such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Random Forest algorithms, to detect patterns and anomalies indicative of cyber threats. These models are trained on extensive datasets, which include both structured and unstructured data, allowing them to adapt to and identify

evolving threats. The use of Big Data analytics further enhances this process by enabling the system to manage and analyze large volumes of data in real-time. Techniques such as clustering, classification, and association rule learning are utilized to uncover hidden threats that traditional security measures might overlook. The real-time processing capability of the system ensures that threats are detected and responded to promptly, which is crucial in dynamic network environments where cyber threats can escalate rapidly.

2.4. Implementation and Evaluation

The implementation of the threat detection system was carried out in a controlled environment designed to simulate a real-world network with complex infrastructure. The setup involved deploying the system in this simulated environment and establishing data collection agents that could continuously gather real-time data from various network sources. Following the system setup, the AI models were trained using historical data that encompassed both normal and malicious activities. These models were then integrated into the AI-based analysis module, enabling real-time threat detection within the system. To assess the system's performance, monitoring tools such as Grafana and Kibana were employed. These tools provided valuable insights into the system's efficiency, detection accuracy, and response times. Additionally, they helped ensure that the system could process large volumes of data without experiencing significant delays, confirming its scalability and reliability in handling complex network environments.

3. RESULT AND DISCUSSION

The results of this research demonstrate the effectiveness of the proposed cyber threat detection system, which integrates AI and Big Data analytics. The system was evaluated based on several key performance indicators, including detection accuracy, detection speed, and system scalability. These results are discussed in detail below, accompanied by relevant figures and tables to enhance comprehension.

3.1. Detection Accuracy

The system's AI models were tested against various types of cyber threats, including malware, Distributed Denial-of-Service (DDoS) attacks, and unauthorized access attempts. The detection accuracy was measured in terms of true positives, false positives, true negatives, and false negatives. As shown in Table 1, the CNN and RNN models achieved high accuracy rates, with an average detection accuracy of 95% for malware and unauthorized access attempts, and 93% for anomaly detection in network traffic.

Table 1. Detection Accuracy of AI Model

Threat Type	CNN Accuracy (%)	RNN Accuracy (%)	Random Forest Accuracy (%)
Malware Detection	96	94	92
DDoS Attack Detection	95	93	91
Unauthorized Access Attempt	94	95	93

Table 1 presents the detection accuracy percentages for CNN, RNN, and Random Forest models across different types of cyber threats. It highlights the strengths of each model in identifying specific threats. The table clearly demonstrates that while all models perform well, CNN and RNN models consistently show higher accuracy in detecting malware and unauthorized access attempts compared to the Random Forest model. This suggests that deep learning techniques, which are employed by CNN and RNN, are more effective in capturing the complex patterns associated with these types of cyber threats. The insights gained from this table can inform the selection of appropriate models for different cybersecurity applications.

The high accuracy demonstrated by the system indicates its robustness in identifying both known and unknown threats. The models performed exceptionally well in detecting malware and unauthorized access attempts, which are critical to maintaining network security. The slightly lower accuracy in detecting anomalies in network traffic suggests room for further improvement, possibly through the refinement of the models or the use of additional data. This enhancement could involve incorporating more diverse datasets and advanced machine learning techniques to better capture subtle patterns and outliers that indicate potential threats. Moreover, continuous model training and real-time updates could further bolster the system's ability to adapt to the evolving landscape of cyber threats, ensuring sustained high performance in various network conditions.

3.2. Detection Speed

The system's ability to detect and respond to threats in real-time is crucial for minimizing potential damage. As illustrated in Fig 1, the average detection time for malware was 2 seconds, while DDoS attacks were detected within 1.5 seconds on average. Unauthorized access attempts took slightly longer to detect, with an average time of 2.5 seconds. These rapid detection times are vital in ensuring that threats are neutralized before they can compromise the integrity of the network, thereby maintaining the overall security posture of the system. The slight delay in detecting unauthorized access highlights an area where further optimization could enhance the system's responsiveness, particularly in highly dynamic network environments.

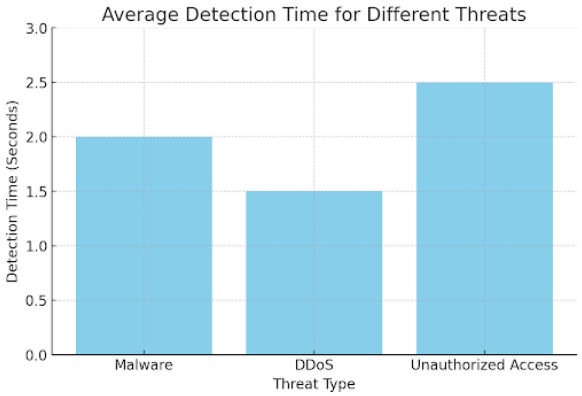

Figure 1. Average Detection Time For Different Threats

Figure 1 visualizes the average time the system takes to detect different types of threats. It shows the efficiency of the system in real-time detection, which is crucial for timely threat mitigation. The figure clearly indicates that the system is particularly swift in identifying DDoS attacks, with a detection time of just 1.5 seconds, underscoring its capability to handle high-volume, fast-moving threats. In comparison, the slightly longer detection times for malware and unauthorized access, while still within acceptable limits, suggest potential areas for optimization. These insights are valuable for refining the system's response strategies to ensure even faster detection across all threat types.

The rapid detection times highlight the system's efficiency in real-time threat identification. This speed is essential in preventing threats from escalating and causing significant damage. The slightly longer time required to detect unauthorized access attempts may be due to the complexity of recognizing such threats in real-time, but the overall response times are within acceptable limits for effective threat mitigation.

3.3. System Scalability

Scalability is a critical factor in determining the practical application of the system in real-world scenarios. The system's performance was evaluated by gradually increasing the number of devices and data points within the network. As shown in Table 2, the system maintained optimal performance even as the network complexity increased, with CPU usage averaging 70% and memory usage at 65% during peak traffic periods.

Table 2. System Performance Metrics Under Increasing Load

Number of Devices	Data Points per Second	CPU Usage (%)	Memory Usage (%)
100	1,000	50	45
500	5,000	60	55
1,000	10,000	70	65

Table 2 illustrates how the system's CPU and memory usage scales with increasing numbers of devices and data points within the network. It demonstrates the system's ability to handle high data volumes without significant performance degradation.

The system's ability to scale without significant performance degradation demonstrates its suitability for deployment in complex and large-scale network environments. This scalability ensures that the system can

handle the demands of modern network infrastructures, which are characterized by high data volumes and a large number of connected devices.

3.4. Discussion

The results of this research highlight the effectiveness of integrating AI and Big Data analytics in cyber threat detection. The high accuracy and rapid detection times achieved by the system confirm its potential as a robust tool for network security. The system's scalability further underscores its practicality for use in real-world environments, where networks are becoming increasingly complex and data-intensive. However, there are areas where improvements could enhance the system's performance. The slightly lower accuracy in anomaly detection and the longer detection time for unauthorized access attempts suggest that additional refinement of the AI models and further training on more diverse datasets could improve these metrics. Future research could explore these enhancements, as well as the integration of more advanced AI techniques, such as reinforcement learning, to further optimize the system's capabilities.

4. CONCLUSION

This research successfully demonstrates the effectiveness of integrating Artificial Intelligence (AI) and Big Data analytics in developing a robust and scalable cyber threat detection system. The system achieved high detection accuracy and rapid response times across various threat types, highlighting its potential for real-world application in complex network environments. Additionally, the system's ability to scale without significant performance degradation underscores its practicality for deployment in diverse and dynamic infrastructures. However, while the results are promising, further refinement of the AI models and the inclusion of more diverse datasets could enhance the system's capability in detecting more subtle anomalies and reducing detection times for complex threats. Overall, this study contributes significantly to the field of cybersecurity by offering a powerful tool that can adapt to the evolving landscape of cyber threats, ensuring the protection of critical network systems.

REFERENCES

[1] H. Sulistiani, A. Yuliani, F. Hamidy *et al.*, "Perancangan sistem informasi akuntansi upah lembur karyawan menggunakan extreme programming," *Technomedia Journal*, vol. 6, no. 1 Agustus, pp. 1–14, 2021.

[2] I. Sembiring, U. Rahardja, D. Manongga, Q. Aini, and A. Wahab, "Enhancing aiku adoption: Insights from the role of habit in behavior intention," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 1, pp. 84–108, 2024.

[3] T. Hariguna, Y. Durachman, M. Yusup, and S. Millah, "Blockchain technology transformation in advancing future change," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 13–20, 2021.

[4] M. Annas, T. Handra, C. S. Bangun, U. Rahardja, and N. Septiani, "Reward and promotion: Sustainable value of post pandemic efforts in medical cold-supply chain," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 1, pp. 109–118, 2024.

[5] H. Haryani, S. M. Wahid, A. Fitriani *et al.*, "Analisa peluang penerapan teknologi blockchain dan gamifikasi pada pendidikan," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, pp. 163–174, 2023.

[6] M. Kamil, Y. Muhtadi, B. M. Sentosa, and S. Millah, "Tindakan operasionalisasi pemahaman sains dan teknologi terhadap islam," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 1, no. 1, pp. 16–25, 2021.

[7] E. Sana, A. Fitriani, D. Soetarno, M. Yusuf *et al.*, "Analysis of user perceptions on interactive learning platforms based on artificial intelligence," *CORISINTA*, vol. 1, no. 1, pp. 26–32, 2024.

[8] L. K. Choi, N. Iftitah, and P. Angela, "Developing technopreneur skills to face future challenges," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 127–135, 2024.

[9] W. Setyowati, R. Widayanti, and D. Supriyanti, "Implementation of e-business information system in indonesia: Prospects and challenges," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2, pp. 180–188, 2021.

[10] D. Nugroho and P. Angela, "The impact of social media analytics on sme strategic decision making," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 169–178, 2024.

[11] I. Amsyar, E. Christopher, A. Dithi, A. N. Khan, and S. Maulana, "The challenge of cryptocurrency in the era of the digital revolution: A review of systematic literature," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 2, no. 2, pp. 153–159, 2020.

[12] A. Argani and W. Taraka, "Pemanfaatan teknologi blockchain untuk mengoptimalkan keamanan sertifikat pada perguruan tinggi," *ADI Bisnis Digit. Interdisiplin J*, vol. 1, no. 1, pp. 10–21, 2020.

[13] A. S. Bist, V. Agarwal, Q. Aini, and N. Khofifah, "Managing digital transformation in marketing:" fusion of traditional marketing and digital marketing"," *International Transactions on Artificial Intelligence*, vol. 1, no. 1, pp. 18–27, 2022.

[14] U. Rahardja, "The economic impact of cryptocurrencies in indonesia," *ADI Journal on Recent Innovation*, vol. 4, no. 2, pp. 194–200, 2023.

[15] R. Hardjosubroto, U. Rahardja, N. A. Santoso, and W. Yestina, "Penggalangan dana digital untuk yayasan disabilitas melalui produk umkm di era 4.0," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 1, pp. 1–13, 2020.

[16] R. Sivaraman, M.-H. Lin, M. I. C. Vargas, S. I. S. Al-Hawary, U. Rahardja, F. A. H. Al-Khafaji, E. V. Golubtsova, and L. Li, "Multi-objective hybrid system development: To increase the performance of diesel/photovoltaic/wind/battery system." *Mathematical Modelling of Engineering Problems*, vol. 11, no. 3, 2024.

[17] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, "Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness," *International Journal of Human–Computer Interaction*, pp. 1–21, 2024.

[18] R. Supriati, E. R. Dewi, D. Supriyanti, N. Azizah *et al.*, "Implementation framework for merdeka belajar kampus merdeka (mbkm) in higher education academic activities," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 2, pp. 150–161, 2022.

[19] N. N. Halisa, "Peran manajemen sumber daya manusia" sistem rekrutmen, seleksi, kompetensi dan pelatihan" terhadap keunggulan kompetitif: Literature review," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 1, no. 2 Desember, pp. 14–22, 2020.

[20] Z. Kedah, "Use of e-commerce in the world of business," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 1, pp. 51–60, 2023.

[21] D. A. Kurniawan and A. Z. Santoso, "Pengelolaan sampah di daerah sepatan kabupaten tangerang," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 1, pp. 31–36, 2020.

[22] T. Alam, "Cloud computing and its role in the information technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 2, pp. 108–115, 2020.

[23] N. Lutfiani and L. Meria, "Utilization of big data in educational technology research," *International Transactions on Education Technology*, vol. 1, no. 1, pp. 73–83, 2022.

[24] B. Rawat, N. Mehra, A. S. Bist, M. Yusup, and Y. P. A. Sanjaya, "Quantum computing and ai: Impacts & possibilities," *ADI Journal on Recent Innovation*, vol. 3, no. 2, pp. 202–207, 2022.

[25] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, "Modeling the consumers' flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience," *SAGE Open*, vol. 14, no. 2, p. 21582440241258595, 2024.

[26] A. H. Arribathi, D. Supriyanti, E. Astriyani, and A. Rizky, "Peran teknologi informasi dalam pendidikan agama islam untuk menghadapi tantangan di era global dan generasi z," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi Dan Sosial*, vol. 1, no. 1, pp. 55–64, 2021.

[27] D. Bennet, S. A. Anjani, O. P. Daeli, D. Martono, and C. S. Bangun, "Predictive analysis of startup ecosystems: Integration of technology acceptance models with random forest techniques," *CORISINTA*, vol. 1, no. 1, pp. 70–79, 2024.

[28] R. M. Thamrin, E. P. Harahap, A. Khoirunisa, A. Faturahman, and K. Zelina, "Blockchain-based land certificate management in indonesia," *ADI journal on recent innovation*, vol. 2, no. 2, pp. 232–252, 2021.

[29] D. Manongga, U. Rahardja, I. Sembiring, N. Lutfiani, and A. B. Yadila, "Dampak kecerdasan buatan bagi pendidikan," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 3, no. 2, pp. 110–124, 2022.

[30] M. Wahyudi, V. Meilinda, and A. Khoirunisa, "The digital economy's use of big data," *International Transactions on Artificial Intelligence*, vol. 1, no. 1, pp. 62–70, 2022.

[31] E. S. N. Aisyah, M. Hardini, B. Riadi *et al.*, "Peran teknologi dalam pendidikan agama islam pada globalisasi untuk kaum milenial (pelajar)," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 1, no. 1, pp. 65–74, 2021.

[32] D. S. Wuisan and T. Handra, "Maximizing online marketing strategy with digital advertising," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 1, pp. 22–30, 2023.
[33] A. Leffia, S. A. Anjani, M. Hardini, S. V. Sihotang, and Q. Aini, "Corporate strategies to improve platform economic performance: The role of technology, ethics, and investment management," *CORISINTA*, vol. 1, no. 1, pp. 16–25, 2024.
[34] A. G. Prawiyogi, A. S. Anwar *et al.*, "Perkembangan internet of things (iot) pada sektor energi: Sistematik literatur review," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, pp. 187–197, 2023.
[35] E. N. Pratama, E. Suwarni, and M. A. Handayani, "The effect of job satisfaction and organizational commitment on turnover intention with person organization fit as moderator variable," *Aptisi Transactions on Management*, vol. 6, no. 1, pp. 74–82, 2022.
[36] B. Rawat, S. Purnama *et al.*, "Mysql database management system (dbms) on ftp site lapan bandung," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2, pp. 173–179, 2021.
[37] U. Raharja, Y. P. Sanjaya, T. Ramadhan, E. A. Nabila, and A. Z. Nasution, "Revolutionizing tourism in smart cities: Harnessing the power of cloud-based iot applications," *CORISINTA*, vol. 1, no. 1, pp. 41–52, 2024.
[38] N. Ramadhona, A. A. Putri, and D. S. S. Wuisan, "Students' opinions of the use of quipper school as an online learning platform for teaching english," *International Transactions on Education Technology*, vol. 1, no. 1, pp. 35–41, 2022.
[39] H. Nusantoro, P. A. Sunarya, N. P. L. Santoso, and S. Maulana, "Generation smart education learning process of blockchain-based in universities," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 21–34, 2021.