INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

AI-Driven Threat Detection and Response Systems for Secure National Infrastructure Networks: A Comprehensive Review

[1]Akinkunle Akinloye., [2]Sunday Anwansedo and [*3]Oladayo Tosin Akinwande

[1]MTN Nigeria, Ltd.

[2]Southern University and A & M College, United State.

[3]Veritas University, Bwari Abuja, Nigeria.

[*]Corresponding Author

DOI: https://doi.org/10.51583/IJLTEMAS.2024.130710

Received: 01 June 2024; Revised: 21 June 2024; Accepted: 01 July 2024; Published: 05 August 2024

Abstract: Due to the increased complexity and damage of cyberattacks in this digital age, the security of national infrastructure networks has become a vital concern. However, a possible approach to improve the cybersecurity of these crucial networks is to incorporate artificial intelligence (AI) into threat detection and response systems; to rapidly evaluate large data sets, identify anomalies, and automate countermeasures to lessen the effects of cyberattacks. The impact, implementation and approaches for anomaly detection and response automation of AI-powered solutions for safeguarding national infrastructure are examined in this paper. Understanding how AI technologies are used to automate threat detection and response, reviewing the operational usefulness of AI in enhancing cybersecurity measures and evaluating the deployment of these systems in critical infrastructure settings were also examined. The study revealed that the speed and accuracy of threat detection and response are greatly increased by AI-powered systems. The automation capacity of AI can potentially reduce the need for human analysts, while also providing faster threat mitigation. Additionally, the usefulness of AI across sectors indicates its practicality in situations and how it may adapt in response to new threats. In conclusion, AI-driven threat detection and response systems are an important development in national infrastructure network cybersecurity. Therefore, by improving the capacity to recognize and address cyber-attacks these technologies can ultimately increase the overall resilience of national infrastructures.

Keywords: Artificial Intelligence (AI), Machine Learning, Threat Detection, Response Systems, Network Security

I. Introduction

The reliance on digital infrastructure, and safeguarding national infrastructure networks in modern times is of utmost importance. This growing digitization and interconnectedness of critical infrastructure systems, have increased accessibility and efficiency while also creating new vulnerabilities (Daniel & Segun, 2024). The potential impact of cyber threats has also become a major concern since critical sectors including energy, transportation, telecommunications, and healthcare are becoming more and more dependent on networked networks (Reddy & Reddy 2014).

The security intelligence report by Reed (2023), revealed that the global high-impact attacks on critical infrastructure increased by 140% in 2022, with over 150 occurrences impacting industrial operations. Therefore, effective security systems that can rapidly react to changing threats are essential, as evidenced by cyber threats that are capable of launching persistent and focused attacks. Artificial intelligence (AI) integration into threat detection and response systems has great potential in this regard (Kaur et al., 2023). There are a lot of hazards associated with cyberattacks on national infrastructure networks, from possible economic and societal repercussions to service interruptions and data breaches. Conventional security strategies, which depend on signature-based detection techniques and rule-based systems, may no longer meet the requirements of the evolving digital ecosystem marked by threats (Ghadge, 2024; Liu et al., 2021).

Cybersecurity protects information and communication systems that are accessible over the internet from threats and harmful attacks (Li & Liu, 2021). In recent times, the Fourth Industrial Revolution and the Industrial Internet of Things (IIoT) have expanded the scope of cybersecurity, becoming multidimensional, and encompassing infrastructure, cloud, and information security in addition to network and application security (Yu & Guo, 2019). Therefore, cybersecurity comprises system security; a variety of interconnected technologies and components in cyberspace. Cybersecurity in an organizational setting entails concurrently safeguarding all pertinent cyberspace dimensions (Li & Liu, 2021).

The most common kind of AI in organizational cyber security, machine learning (ML), has emerged due to developments in data science and computer science (Scott & Kyobe, 2021). ML is the ability of a machine to learn and adapt through experience It is considered a subset of AI that concentrates on the application of specific system types that can learn from past data to find patterns and make decisions autonomously (Wazid et al., 2022). Numerous ML applications in cyberspace, such as threat intelligence, anomaly detection, and task automation for cybersecurity, can be facilitated by the enormous volumes of data that organizations generate (Huang & Rust, 2018). Generally, adopting threat detection and response systems driven by AI is not without its challenges (Rizvi, 2023). There are many obstacles to overcome, including issues with data availability and quality, model interpretability, algorithm bias, and adversarial attacks. Furthermore, issues with dependability, privacy, and other

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

unforeseen repercussions arise when AI is included in critical infrastructure (Paras, 2023). Understanding the technological, organizational, and regulatory aspects of AI-driven cybersecurity solutions is necessary to holistically address these problems. The purpose of this paper is to provide an in-depth review of AI-powered methods for protecting national infrastructure networks from online attacks. This review explores the impact of AI on cybersecurity within national infrastructure, AI approaches for threat detection and response automation, AI systems, and relevant implementation in critical infrastructure settings including operational assessments demonstrating the effectiveness of AI as well as potential applications of AI-driven security technologies in protecting critical infrastructure.

II. Impact of AI on National Infrastructure Cybersecurity

Although the idea of AI in cybersecurity is not entirely novel, it has recently acquired prominence as a result of the complexity and frequency of rising cyberattacks, as well as the volume and diversity of data and devices that are to be safeguarded. The invention and adoption of other cutting-edge technologies, such as cloud, quantum, edge computing, blockchain, IoT, optical networks and 5G, which provide new security concerns as well as opportunities, also have an impact on AI in cybersecurity (Singh S. K. et al., 2021). Consequently, AI in cybersecurity is a dynamic and developing issue requiring continuous research and collaboration. The widely recognized cybersecurity framework by NIST is to assist in comprehending the several categories required to safeguard, identify, respond to, and repel cyberattacks (Barrett, 2018). The fundamentals of the NIST cybersecurity framework outline how to strengthen an organization's cybersecurity (*Figure 1*).

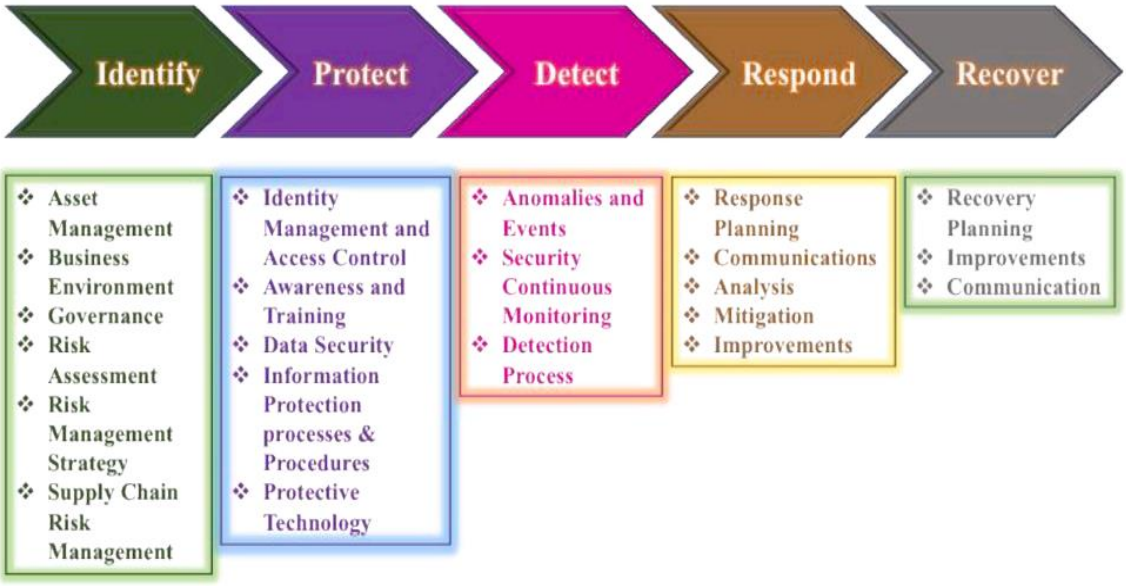

Figure 1. Cybersecurity framework by NIST

The preliminary phases of AI in cybersecurity were centered on anomaly detection and intrusion prevention systems. This is represented by the 1990s–2000s. The ML era began in the 2010s until the present times (Audibert et al., 2022). The emergence of ML algorithms revolutionized AI-powered cybersecurity solutions by enabling more sophisticated threat identification, analysis, and prediction (Mohamed, 2023). The 2020s and beyond saw the development of deep learning techniques, which further enhanced AI capabilities and allowed for more complex and nuanced threat analysis, such as identifying hidden patterns in cyberattacks and identifying zero-day attacks (Aslan et al., 2023).

Large volumes of data from many sources are analyzed by AI algorithms, allowing for the proactive detection of even the most subtle dangers. Processes related to incident response, including containment, remediation, and recovery, can be automated by AI systems, greatly speeding up reaction times (Chahal, 2023). AI models forecast potential cyberattacks by examining past data and present trends. This allows for proactive mitigation techniques and resource allocation. AI technologies can improve the efficacy and efficiency of security solutions by tailoring them to particular threats and situations. AI can help close the talent gap in cybersecurity by automating repetitive processes and enhancing human knowledge (Tonhauser & Ristvej, 2023).

Since AI enables machines to carry out tasks including learning, thinking, and decision-making that traditionally need human intelligence, AI has the potential to be an essential tool in safeguarding the national infrastructure of a country, which includes things like electricity, water, transportation, and communication systems and assets that are necessary for a country to function and be secure (Ghosh et al., 2018). By utilizing data analytics, ML, and natural language processing to find patterns, anomalies, and vulnerabilities that can point to malicious activity or possible threats, AI can assist in the detection and prevention of cyberattacks on critical infrastructure. AI may also improve and automate the handling of security incident response and remediation through the use of preset workflows, policies, and rules. With the use of sensors, computer vision, and deep learning,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

AI can monitor and manage both the digital and physical components of infrastructure, including traffic lights, power grids, and pipelines. This can assist optimize the resilience and performance of essential infrastructure (McMillan & Varga, 2022). AI can also be used to anticipate and lessen the effects of man-made and natural disasters, like fires, floods, and earthquakes, on infrastructure (Şimşek et al., 2023). AI can create and revolutionize infrastructure by employing image recognition, pattern recognition, and data mining to identify and take advantage of new opportunities and problems for the infrastructure, such as renewable energy sources, smart cities, and IoT devices, AI may help innovate and alter essential infrastructure.

AI presents a variety of dangers and problems, including those related to data quality, privacy, security, ethics, and governance, but it can also provide several advantages and chances for enhancing the sustainability, efficiency, and security of the national infrastructure (Ade-Ibijola & Okonkwo, 2023). Therefore, it is critical to ensure AI is developed and utilized in a way that supports infrastructure norms, human rights, and transparency while also being inclusive Modern society is anchored by its national infrastructure, which includes critical systems like water treatment plants, transportation networks, energy grids, and communication systems (Robbins & van Wynsberghe, 2022). To ensure public safety, economic growth, and national security, this infrastructure must be protected from cyberattacks and other threats. Artificial intelligence (AI) is showing great promise in several areas and is becoming a potent instrument for bolstering the security and resilience of the country's infrastructure.

Large volumes of data from sensors, cameras, and network traffic are analyzed by AI algorithms, which then detect anomalies and possible risks that would go undetected by humans. By recognizing tiny patterns that point to malicious behaviour and detecting zero-day attacks, ML models can learn from and adapt to evolving threats (Thwaini, 2022). Threat intelligence solutions driven by AI gather and evaluate threat data from many sources, giving digital security professionals a thorough situational awareness. AI makes it possible to perform preventative maintenance and save downtime by anticipating potential infrastructure risks and equipment problems before they happen. AI-driven risk assessment models identify locations most vulnerable to interruptions by analyzing a variety of variables, including traffic patterns, weather, and historical data (Gkioka et al., 2024; Ghaffarian et al., 2023). Resource allocation and reaction planning are made possible by predictive analytics, which also helps to reduce risks and potential harm from incidents (Aven, 2016).

Yaacoub et al., (2021) revealed that aspects of incident response that can be automated by AI systems include fast resuming operations, containing threats, and isolating impacted systems. Security teams may reduce disruption during cyberattacks, optimize resource allocation, and prioritize responses with the aid of AI-powered decision support technologies. Infrastructure that is capable of self-healing can automatically identify and fix small problems, decreasing the need for human intervention and enhancing resilience. Intrusion detection systems with AI capabilities can recognize and stop illegal access attempts, shielding vital systems from online threats (Markevych & Dawson, 2023). Algorithms for behavioural analysis can recognize possible insider threats and identify unusual user behaviour. Access control to critical infrastructure components can be made more effective and safer with the use of AI-based authentication and authorization systems.

III. AI Approaches for Anomaly Detection and Response Automation

Maintaining an effective defense against cyber threats requires being able to recognize potential vulnerabilities in cyber security. AI enables organizations access to advanced features that extend beyond conventional approaches, enabling them to strengthen their security (Jada & Mayayise, 2023).

Anomaly Detection

AI systems are highly effective at identifying anomalies in behaviour, which serves as a vital barrier against cyber-attacks. The foundation of this strategy is the creation of baselines, a dynamic process whereby AI continuously picks up knowledge and keeps an eye on the intricate web of user and system activity in a cloud environment (Samariya & Thakkar, 2021). It is necessary to properly construct baselines that include typical behaviour inside the cloud ecosystem so as to influence the anomalous capabilities of AI. AI can identify common patterns and interactions between individuals, systems, and applications through ongoing observation and learning. Therefore, comprehension enables prompt identification of deviations that can indicate possible security risks.

Moreover, ongoing analysis of user behaviours, network activity, and system processes enables AI systems to improve and modify their conception of normalcy, guaranteeing that the baseline continues to be applicable even when user patterns and system configurations change (Alanazi & Aljuhani, 2023). AI gets proficient at swiftly spotting anomalies, or the unanticipated departures from acquired norms, once the baselines are set. However, anomalies might manifest themselves in a variety of ways, such as irregular data transfers or strange access patterns. The speed at which AI-driven anomaly detection operates is crucial because it allows quick identification of possible dangers, such as zero-day assaults, that would have been impossible to detect using more conventional methods. Consequently, through learning and adjusting to typical behaviour, AI systems can identify deviations that correspond with the characteristics of zero-day attacks. These deviations may include anomalous network traffic, unexpected data access, or aberrant system behaviour, all of which can serve as warning signs of impending danger.

Response Automation

According to Tatineni (2023), AI expedites recovery times and minimizes damage by streamlining incident response procedures. AI can accomplish this considering that it can recognize and react to threats rapidly, therefore making this component of security

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

automation and incident response more effective and enabling smooth, advanced threat detection and response in cloud security. In addition, the rapid threat detection and reaction of AI reduces the effect of security issues without requiring human participation. AI, for instance, may swiftly and effectively respond to new threats by automatically quarantining infected devices or undoing modifications initiated by cyber criminals.

Furthermore, security automation also includes a wide range of routine and repetitive security duties that are easy for humans to overlook. These include setting up firewalls, running malware scans, reacting to notifications, fixing vulnerabilities, and changing passwords (Settanni, 2022). The cyber security teams may concentrate on higher-value duties like threat hunting, constant monitoring, and improving the overall security status when these security operations are automated using AI and relieved of routine tasks. AI-driven automation relieves the teams of these tedious activities, which speeds up response times and lowers the chance of mistakes, resulting in a more flexible and effective security framework and promoting ongoing security improvement.

IV. AI Implementation and Effectiveness in Critical Infrastructure Systems

Each of the four infrastructure sectors: transportation, water, energy, communications, military, and finance utilize AI distinctively. The implementation, application, and effectiveness of AI techniques in each sector are covered in this section.

Transportation

Abduljabbar et al., (2019) revealed that the most varied range of tasks to which AI has been applied has been found in the transport sector. When considering transport networks as a whole, several ontology-based knowledge representation systems have been proposed (Bouhana et al., 2015). Additionally, a variety of ML techniques have been useful in recent research on how the public interacts with transport systems from a behavioural perspective, including the selection of transport modes (Koushik et al., 2020). While it is acknowledged that traffic flow and accident prediction can be used in several urban transportation systems (Doğan and Akgüngör, 2011, Zhang et al., 2020), the majority of the remaining research in this field has concentrated on individual transportation modes.

Concerning the use of road vehicles, various ML techniques have been used for navigational tools (Veres & Moussa, 2020), traffic (Jiang & Zhang, 2019), and accident forecasting (Ren et al., 2018). Comparable instruments have also been employed in destination prediction for taxi services (Veres and Moussa, 2019) and demand prediction (Yao et al., 2018). While Šegvić et al., (2010) proposed computer vision-based techniques for traffic infrastructure monitoring, other researchers have attempted to use AI in the identification and mapping of road networks (Ekpenyong et al., 2009). Deep learning techniques are expected to be important in the creation of an intelligent transport network, with Convolutional Neural Networks (CNNs) being used in object detection, localization, and classification for a variety of applications. In-vehicle and roadside sensors have the potential to provide more data on road networks than ever before (Sirohi et al., 2020). In recent years, there has been a great deal of interest in the development of self-driving cars. Computer vision, machine and deep learning, automated reasoning, and other methods have all been applied to this mostly robotics-based challenge (Ma et al., 2020). AI has been used in transportation in areas other than roadways. Even while robotics, particularly unmanned aerial vehicles (UAVs), show great promise for railway asset monitoring, many still rely heavily on human contact (Flammini et al., 2016). However, deep learning technologies have shown themselves to be useful for diagnosing faults in high-speed rail, which is predicted to become a more common means of transportation (Yin and Zhao, 2016). Individual research by Mendes-Moreira et al., (2015) on bus networks has mostly focused on scheduling challenges, whereas the majority of other work in public transport has primarily focused on traffic flows or choice of transportation method (Koushik et al., 2020).

Military

The study by Bhardwaj (2023) revealed that projections regarding the use of AI in military applications, and several important advanced military technologies will either be redefined or defined over the coming years. Intelligent AI solutions will mostly arise from the combination of knowledge-focused and analytical skills. The AI solutions will then be connected to fully utilize the advantages of blockchain technology concerning data integrity and to influence the network of physical and virtual domains, which will comprise sensors, organizations, people, and autonomous agents. In line with predictions made by the NATO Science and Technology Organization (2020), this comprises digitally merging the physical, informational, and human fields to support new disruptive effects; disperse over a sizable region and utilize large-scale, decentralized sensor networks, storage, and processing.

The uses of AI such as chatbots, automated drones, virtual assistants, facial recognition, cognitive automation, fraud detection, autonomous vehicles, and predictive analytics applications have a common feature. *Figure 2* illustrates how, despite the wide range of applications, experts who have developed numerous AI projects are aware that each AI use case fits into one or more of these seven categories. Goal-driven systems, autonomous systems, conversational/human interfaces, hyper personalization, predictive analytics, and decision support are the seven patterns of artificial intelligence. These seven AI patterns have transformed military operations in the last few years by bringing new capabilities and uses for activities including conversational interactions, decision support, and object recognition. Let's examine a small portion of the seven AI patterns in the military, emphasizing current developments and academic research in each field.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

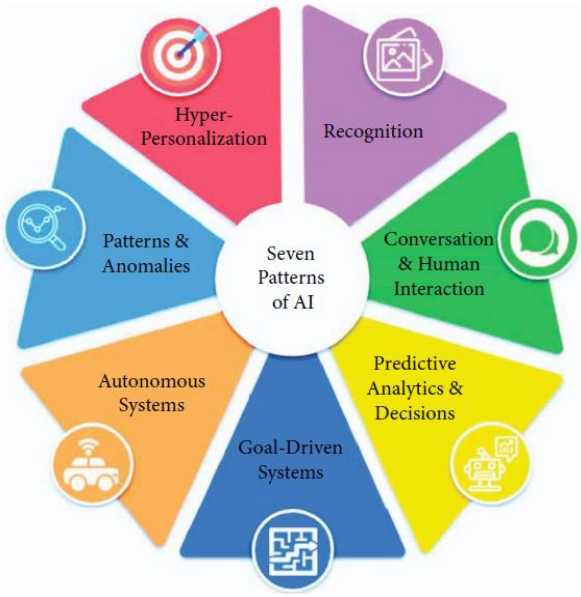

Figure 2. The seven AI patterns (Rashid A. B. et al., 2023)

On battlefields, AI is becoming more common. Similar to corporations and sectors, the military is gradually beginning to focus more on AI in its advancement and development. Military systems with AI capabilities can handle massive amounts of data faster than traditional systems. Additionally, through natural computation and decision-making skills, AI improves the self-actuation, self-regulation, and self-control of flying systems. *Figure 3*, shows the AI capabilities important to military operations for simplicity and their applications in defence sectors. Most military applications involve AI, and growing military support for innovative and advanced AI technologies is anticipated to increase the demand for AI-driven systems in the military (Taddeo et al., 2021).

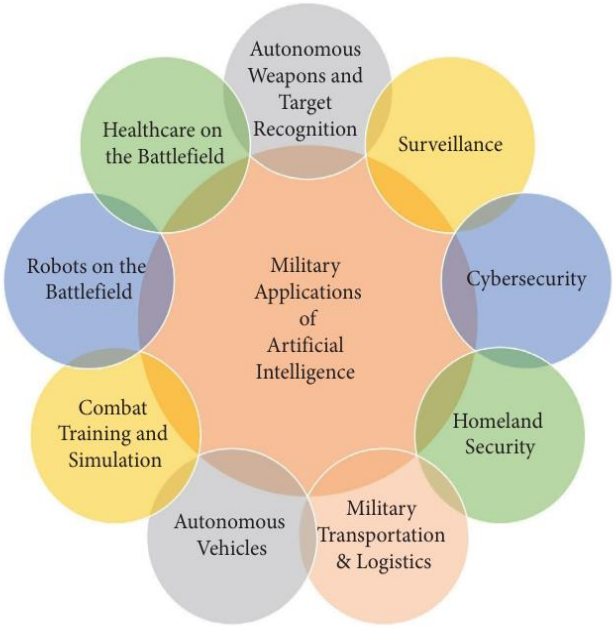

Figure 3. AI applications in the defence sector (Rashid A. B. et al., 2023)

Finance

Integration of AI in the financial market has gained popularity, due to the potential to revolutionize the financial industry (Maple et al., 2023). The advanced computational methods, including ML, natural language processing, and predictive analytics of AI allow systems to examine large volumes of data, identify trends, and make well-informed decisions without the need for explicit human programming. AI applications have demonstrated the potential to improve risk management, increase efficiency, and

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

increase accessibility to financial services in the context of financial markets, especially in emerging economies where conventional infrastructures may be lacking (Ochuba et al., 2024).

Furthermore, AI plays a role in expanding financial services accessibility, especially in developing nations. AI-driven solutions are empowering people and communities, promoting economic growth, and propelling social development through democratizing access, personalizing guidance, and increasing inclusiveness. The ability of AI to solve accessibility issues and spur innovation in the financial services sector will only increase as these technologies develop and become more advanced (Kang et al., 2020). This will completely transform the sector and open up new avenues for financial inclusion and empowerment.

Water

Water networks have used AI techniques for anything from early water treatment to distribution and customer-related issues. On the supply side, a large portion of research has focused on pollutant removal (Fan et al., 2018) and water quality, in both potable and wastewater treatment (Granata et al., 2017, Li et al., 2021). Al Aani et al. (2019) have reported that ML techniques have been applied in the desalination process, with potential consequences for the design of water plants. From the viewpoint of end-users, a variety of machine learning techniques, such as Artificial Neural Networks (ANNs), Random Forests (RFs), Support Vector Machines (SVMs), regression trees, and Deep Belief Networks (DBNs), have been applied to price forecasting (Xu et al., 2019) and water demand forecasting (Antunes et al., 2018) across a range of geographic scales.

Energy

AI tools have been widely used in the energy sector for demand forecasting, particularly at the residential and building levels (Mocanu et al., 2016, Ahmad et al., 2014, Mat Daut et al., 2017). Demand-side management and price forecasting are two other uses (Macedo et al., 2015; Ghoddusi et al., 2019). In this industry, facilitating the reduction of energy use is becoming more and more important. In general, a variety of techniques have been used, from efficiency-centered ontologies to natural language creation of consumer advice reports (Tomic et al., 2010; Conde-Clemente et al., 2018). The majority of the remaining energy sector activity revolves around generating systems, with many of the most advanced applications relating to infrastructure for renewable energy sources. Although the oil, gas, and nuclear industries can benefit greatly from robotics, the current generation of robots has limited autonomy (Shukla and Karki, 2016). In recent times, AI in renewable energy systems for supply forecasting, with ANN techniques widely used in meteorological forecasting (Suganthi et al., 2015), and in solar tracking (Carballo et al., 2019).

Communication Networks

According to Wang et al., (2020), the efficiency of wireless networks in the future is thought to be dependent on machine learning techniques A variety of networks such as cellular or wireless, 5G, optical, software-defined networks (SDNs) and cloud have been discussed by Li et al., (2017), optical networks, software-defined networks and the cloud (Mata et al., 2018; Gulenko et al., 2016).

Generally, transmission quality and user experience are critical therefore, Casas et al., (2017) and Mata et al., (2018) investigated the assessment of customer experience and network quality, which can be influenced by characteristics such as latency, loss rate, and picture or video definition using relevant ML techniques. However, security remains crucial, particularly with wireless and SDN telecommunications (Lv et al., 2021). Therefore, ML techniques have been applied to the detection of anomalies, identification of intrusion attacks, and choosing suitable responses.

V. Limitations and Ethical Consideration

There are various ethical concerns with the use of AI in critical infrastructure. Inadvertently maintaining biases found in training data can result in unjust or discriminatory outcomes for AI systems (Chen et al., 2023). This is especially problematic for national infrastructure since skewed judgements can have far-reaching effects. For example, an AI system may result in unfair scrutiny or unbalanced resource allocation if it disproportionately labels particular locations or demographics as high risk based on biased data.

Implementing AI-driven systems requires a large infrastructural investment. To handle and analyze data in real time, these systems need sophisticated networking infrastructure, large amounts of storage, and high-performance computing resources. Several organizations may find these standards prohibitively expensive, particularly those in the public sector (Umoga et al., 2024). Additionally, there are continual logistical and budgetary difficulties in maintaining and updating this infrastructure to stay up with technology improvements. Partnerships between public and private sector organizations may help remove in removing these obstacles (Alhosani & Alhashmi, 2024). Public-private partnerships can assist in distributing the cost and utilizing the private sector's technological know-how. However, implementing cloud-based solutions can offer flexible and scalable infrastructure, negating the need for significant upfront costs.

Furthermore, due to potential resistance from stakeholders, several parties may object to the installation of AI-driven technologies in critical infrastructure. Automation may cause workers to dread losing their jobs, but managers and other decision-makers may have doubts about the security and efficacy of AI systems (Gavaghan et al., 2021). The success and effectiveness of AI systems as a whole may be impacted by this opposition, which may impede their acceptance and integration. To solve these issues,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

effective change management techniques are crucial (Ross et al., 2023). This entails open communication regarding the advantages and constraints of AI, offering staff members chances for training and upskilling, and incorporating stakeholders in the process of development and execution. Building confidence and lowering opposition can also be accomplished by showcasing the early accomplishments and observable advantages of AI systems.

Conclusion

The use of AI techniques is growing in both capacity and popularity and the incorporation of AI into cybersecurity systems for national infrastructure networks is a revolutionary advancement in protecting vital assets from a constantly evolving array of threats. The increased instrumentation and digitalization of infrastructure systems, which provide data for AI tools, is also expected to drive the growth of AI applications in this domain. By rapidly analyzing large volumes of data and identifying trends and anomalies that can point to malicious activity, AI improves the capacity to recognize and address cyber threats, especially for national infrastructure, where prompt threat detection might avert disastrous outages. AI is an essential component of the safety of critical infrastructure because of its capacity to adapt and learn from novel data, which guarantees cybersecurity measures stay effective against developing threats.

Security technologies driven by AI can therefore potentially protect national infrastructure. Hence, the resilience and dependability of cybersecurity measures are to be improved by developments in AI research, including the creation of more complex algorithms and the integration of AI with other innovative technologies. Furthermore, the increased focus on ethical AI and transparency in AI decision-making can aid in resolving issues with responsibility and bias, ensuring AI technologies are applied in a way that preserves the standards of security and trust.

References

1. Abduljabbar, R., Dia, H., Liyanage, S., & Bagloee, S. A. (2019). Applications of Artificial Intelligence in Transport: An Overview. Sustainability, 11(1), 189. https://doi.org/10.3390/su11010189
2. Ade-Ibijola, A., & Okonkwo, C. (2023). Artificial Intelligence in Africa: Emerging Challenges. Social and Cultural Studies of Robots and AI, 101–117. https://doi.org/10.1007/978-3-031-08215-3_5
3. Ahmad, A. S., Hassan, M. Y., Abdullah, M. P., Rahman, H. A., Hussin, F., Abdullah, H., & Saidur, R. (2014). A review on applications of ANN and SVM for building electrical energy consumption forecasting. Renewable and Sustainable Energy Reviews, 33, 102–109. https://doi.org/10.1016/j.rser.2014.01.069
4. Al Aani, S., Bonny, T., Hasan, S. W., & Hilal, N. (2019). Can machine language and artificial intelligence revolutionize process automation for water treatment and desalination? Desalination, 458, 84–96. https://doi.org/10.1016/j.desal.2019.02.005
5. Alanazi, R., & Aljuhani, A. (2023). Anomaly Detection for Industrial Internet of Things Cyberattacks. Computer Systems Science and Engineering, 44(3), 2361–2378. https://doi.org/10.32604/csse.2023.026712
6. Alhosani K, & Alhashmi, S. M. (2024). Opportunities, challenges, and benefits of AI innovation in government services: a review. Discover Artificial Intelligence, 4(1). https://doi.org/10.1007/s44163-024-00111-w
7. Aminu M., Anawansedo, S., Yusuf Ademola Sodiq, & Oladayo Tosin Akinwande. (2024). Driving Technological Innovation for a Resilient Cybersecurity Landscape. International Journal of Latest Technology in Engineering Management & Applied Science, XIII(IV), 126–133. https://doi.org/10.51583/ijltemas.2024.130414
8. Antunes, A., Andrade-Campos, A., Sardinha-Lourenço, A., & Oliveira, M. S. (2018). Short-term water demand forecasting using machine learning techniques. Journal of Hydro informatics, 20(6), 1343–1366. https://doi.org/10.2166/hydro.2018.163
9. 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. https://doi.org/10.3390/electronics12061333
10. Audibert, R. B., Lemos, H., Pedro, Tavares, A. R., & Lamb, L. C. (2022). On the Evolution of A.I. and Machine Learning: Towards Measuring and Understanding Impact, Influence, and Leadership at Premier A.I. Conferences. https://doi.org/10.48550/arxiv.2205.13131
11. Aven, T. (2016). Risk Assessment and Risk management: Review of Recent Advances on Their Foundation. European Journal of Operational Research, 253(1), 1–13. Science Direct. https://doi.org/10.1016/j.ejor.2015.12.023
12. Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. NIST Cybersecurity Framework. http://dx.doi.org/10.1002/https://dx.doi.org/10.6028/NIST.CSWP.04162018
13. Bhardwaj, M. (2023). AI and Cyber Security with Reference to Military/ Defense. International Journal of Trend in Research and Development, 10(4), 2394–9333. https://www.ijtrd.com/papers/IJTRD26997.pdf
14. Bouhana, A., Zidi, A., Fekih, A., Chabchoub, H., & Abed, M. (2015). An ontology-based CBR approach for personalized itinerary search systems for sustainable urban freight transport. Expert Systems with Applications, 42(7), 3724–3741. https://doi.org/10.1016/j.eswa.2014.12.012
15. Carballo, J. A., Bonilla, J., Berenguel, M., Fernández-Reche, J., & García, G. (2019). New approach for solar tracking systems based on computer vision, low cost hardware and deep learning. Renewable Energy, 133, 1158–1166. https://doi.org/10.1016/j.renene.2018.08.101

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

16. Casas, P., D'Alconzo, A., Wamser, F., Seufert, M., Gardlo, B., Schwind, A., Tran-Gia, P., & Schatz, R. (2017). Predicting QoE in cellular networks using machine learning and in-smartphone measurements. 2017 Ninth International Conference on Quality of Multimedia Experience (QoMEX). https://doi.org/10.1109/qomex.2017.7965687
17. Chahal, S. (2023). AI-Enhanced Cyber Incident Response and Recovery. International Journal of Science and Research, 12(3), 1795–1801. https://doi.org/10.21275/sr231003163025
18. Chen, P., Wu, L., & Wang, L. (2023). AI Fairness in Data Management and Analytics: A Review on Challenges, Methodologies and Applications. Applied Sciences, 13(18), 10258–10258. https://doi.org/10.3390/app131810258
19. Conde-Clemente, P., Alonso, J. L., & Gracián Triviño. (2018). Toward automatic generation of linguistic advice for saving energy at home. Soft Comput., 22(2), 345–359. https://doi.org/10.1007/s00500-016-2430-5
20. Daniel, & Segun, S. (2024). EMERGING TRENDS IN CYBERSECURITY FOR CRITICAL INFRASTRUCTURE PROTECTION: A COMPREHENSIVE REVIEW. Computer Science & IT Research Journal, 5(3), 576–593. https://doi.org/10.51594/csitrj.v5i3.872
21. Doğan, E., & Akgüngör, A. P. (2011). Forecasting highway casualties under the effect of railway development policy in Turkey using artificial neural networks. Neural Computing and Applications, 22(5), 869–877. https://doi.org/10.1007/s00521-011-0778-0
22. Ekpenyong, F., Palmer-Brown, D., & Brimi combe, A. (2009). Extracting road information from recorded GPS data using snap-drift neural network. Neurocomputing, 73(1-3), 24–36. https://doi.org/10.1016/j.neucom.2008.11.032
23. Fan, M., Hu, J., Cao, R., Ruan, W., & Wei, X. (2018). A review on experimental design for pollutants removal in water treatment with the aid of artificial intelligence. Chemosphere, 200, 330–343. https://doi.org/10.1016/j.chemosphere.2018.02.111
24. Flammini, F., Pragliola, C., & Smarra, G. (2016, November 1). Railway infrastructure monitoring by drones. IEEE Xplore. https://doi.org/10.1109/ESARS-ITEC.2016.7841398
25. GAVAGHAN, C., KNOTT, A., & MACLAURIN, J. (2021). The Impact of Artificial Intelligence on Jobs and Work in New Zealand. https://www.otago.ac.nz/__data/assets/pdf_file/0012/312060/https-wwwotagoacnz-caipp-otago828396pdf-828396.pdf
26. Ghadge, N. (2024). Enhancing threat detection in Identity and Access Management (IAM) systems. International Journal of Science and Research Archive, 11(2), 2050–2057. https://doi.org/10.30574/ijsra.2024.11.2.0761
27. Ghaffarian, S., Taghikhah, F. R., & Maier, H. R. (2023). Explainable artificial intelligence in disaster risk management: Achievements and prospective futures. International Journal of Disaster Risk Reduction, 98, 104123. https://doi.org/10.1016/j.ijdrr.2023.104123
28. Ghoddusi, H., Creamer, G. G., & Rafizadeh, N. (2019). Machine learning in energy economics and finance: A review. Energy Economics, 81, 709–727. https://doi.org/10.1016/j.eneco.2019.05.006
29. Ghosh, A., Chakraborty, D., & Law, A. (2018). Artificial intelligence in Internet of things. CAAI Transactions on Intelligence Technology, 3(4), 208–218. https://doi.org/10.1049/trit.2018.1008
30. Gkioka, G., Dominguez, M., Athina Tympakianaki, & Gregoris Mentzas. (2024). AI-Driven Real-Time Incident Detection for Intelligent Transportation Systems. Advances in Transdisciplinary Engineering. https://doi.org/10.3233/atde240021
31. Granata, F., Papirio, S., Esposito, G., Gargano, R., & De Marinis, G. (2017). Machine Learning Algorithms for the Forecasting of Wastewater Quality Indicators. Water, 9(2), 105. https://doi.org/10.3390/w9020105
32. Gulenko, A., Wall schlager, M., Schmidt, F. I., Kao, O., & Liu, F. (2016). Evaluating machine learning algorithms for anomaly detection in clouds. IEEE International Conference on Big Data (Big Data) (2016), https://doi.org/10.1109/bigdata.2016.7840917
33. Jada, I., & Mayayise, T. O. (2023). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 100063–100063. https://doi.org/10.1016/j.dim.2023.100063
34. Jiang, W., & Zhang, L. (2019). Geospatial data to images: A deep-learning framework for traffic forecasting. Tsinghua Science and Technology, 24(1), 52–64. https://doi.org/10.26599/TST.2018.9010033
35. Kang, Y., Cai, Z., Tan, C.-W., Huang, Q., & Liu, H. (2020). Natural language processing (NLP) in management research: A literature review. Journal of Management Analytics, 7(2), 139–172. https://doi.org/10.1080/23270012.2020.1756939
36. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. Information Fusion, 97(101804), 101804. Science direct. https://doi.org/10.1016/j.inffus.2023.101804
37. Koushik, A. N., Manoj, M., & Nezamuddin, N. (2020). Machine learning applications in activity-travel behaviour research: a review. Transport Reviews, 40(3), 288–311. https://doi.org/10.1080/01441647.2019.1704307
38. Li, L., Rong, S., Wang, R., & Yu, S. (2021). Recent advances in artificial intelligence and machine learning for nonlinear relationship analysis and process control in drinking water treatment: A review. Chemical Engineering Journal, 405, 126673. https://doi.org/10.1016/j.cej.2020.126673

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

39. Li, R., Zhao, Z., Zhou, X., Ding, G., Chen, Y., Wang, Z., & Zhang, H. (2017). Intelligent 5G: When Cellular Networks Meet Artificial Intelligence. IEEE Wireless Communications, 24(5), 175–183. https://doi.org/10.1109/mwc.2017.1600304wc
40. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Reports, 7(7), 8176–8186. Science direct. https://doi.org/10.1016/j.egyr.2021.08.126
41. Liu, Q., Veit Hagenmeyer, & Keller, H. B. (2021). A Review of Rule Learning-Based Intrusion Detection Systems and Their Prospects in Smart Grids. IEEE Access, 9, 57542–57564. https://doi.org/10.1109/access.2021.3071263
42. Lv, Z., Singh, A. K., & Li, J. (2021). Deep Learning for Security Problems in 5G Heterogeneous Networks. IEEE Network, 35(2), 1–8. https://doi.org/10.1109/mnet.011.2000229
43. Ma, Y., Wang, Z., Yang, H., & Yang, L. (2020). Artificial intelligence applications in the development of autonomous vehicles: a survey. IEEE/CAA Journal of Automatica Sinica, 7(2), 315–329. https://doi.org/10.1109/jas.2020.1003021
44. Macedo, M. N. Q., Galo, J. J. M., de Almeida, L. A. L., & de C. Lima, A. C. (2015). Demand side management using artificial neural networks in a smart grid environment. Renewable and Sustainable Energy Reviews, 41, 128–133. https://doi.org/10.1016/j.rser.2014.08.035
45. Maple, C., Szpruch, L., Epiphaniou, G., Staykova, K., Singh, S., & Penwarden, W. (2023). The AI Revolution: Opportunities and Challenges for the Finance Sector. The Alan Turing Institute.
46. Mardanghom, R., Sandal, H., & Xunhua, S. (2019). Artificial Intelligence in Financial Services. https://core.ac.uk/download/pdf/288306886.pdf
47. Markevych, M., & Dawson, M. (2023). A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI). International Conference Knowledge Based Organization, 29(3), 30–37. https://doi.org/10.2478/kbo-2023-0072
48. Mat Daut, M. A., Hassan, M. Y., Abdullah, H., Rahman, H. A., Abdullah, M. P., & Hussin, F. (2017). Building electrical energy consumption forecasting analysis using conventional and artificial intelligence methods: A review. Renewable and Sustainable Energy Reviews, 70, 1108–1118. https://doi.org/10.1016/j.rser.2016.12.015
49. Mata, J., de Miguel, I., Durán, R. J., Merayo, N., Singh, S. K., Jukan, A., & Chamania, M. (2018). Artificial intelligence (AI) methods in optical networks: A comprehensive survey. Optical Switching and Networking, 28, 43–57. https://doi.org/10.1016/j.osn.2017.12.006
50. McMillan, L., & Varga, L. (2022). A review of the use of artificial intelligence methods in infrastructure systems. Engineering Applications of Artificial Intelligence, 116. https://doi.org/10.1016/j.engappai.2022.105472
51. Mendes-Moreira, J., Moreira-Matias, L., Gama, J., & Freire de Sousa, J. (2015). Validating the coverage of bus schedules: A Machine Learning approach. Information Sciences, 293, 299–313. https://doi.org/10.1016/j.ins.2014.09.005
52. Mocanu, E., Nguyen, P. H., Gibescu, M., & Kling, W. L. (2016). Deep learning for estimating building energy consumption. Sustainable Energy, Grids and Networks, 6, 91–99. https://doi.org/10.1016/j.segan.2016.02.005
53. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering, 10(2). https://doi.org/10.1080/23311916.2023.2272358
54. Mohammed Hussein Thwaini. (2022). Anomaly Detection in Network Traffic using Machine Learning for Early Threat Detection. Data & Metadata, 1, 34–34. https://doi.org/10.56294/dm202272
55. Ochuba N. N. A., None Adetumi Adewumi, & Olanrewaju, D. (2024). THE ROLE OF AI IN FINANCIAL MARKET DEVELOPMENT: ENHANCING EFFICIENCY AND ACCESSIBILITY IN EMERGING ECONOMIES. Finance & Accounting Research Journal, 6(3), 421–436. https://doi.org/10.51594/farj.v6i3.969
56. Paras, R. (2023). Ethics in AI: A Deep Dive into Privacy Concerns. https://www.researchgate.net/publication/376517943_Ethics_in_AI_A_Deep_Dive_into_Privacy_Concerns
57. Rashid A. B., Ashfakul Karim Kausik, Hassan, A., & Mehedy Hassan Bappy. (2023). Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges. International Journal of Intelligent Systems, 2023, 1–31. https://doi.org/10.1155/2023/8676366
58. Reddy, N. G., & G. J. Ugander Reddy. (2014). A Study of Cyber Security Challenges and Its Emerging Trends On Latest Technologies. ArXiv.org. https://arxiv.org/abs/1402.1842
59. Reding, D. F., & Eaton, J. (2020). Science & Technology Trends 2020-2040 Exploring the S&T Edge NATO Science & Technology Organization. Http:\Www.sto.nato.int; NATO Science & Technology Organization Office of the Chief Scientist NATO Headquarters B-1110 Brussels Belgium. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf
60. Reed, J. (2023, June 26). High-impact attacks on critical infrastructure climb 140%. Security Intelligence. https://securityintelligence.com/news/high-impact-attacks-on-critical-infrastructure-climb-140/
61. Ren, H., Song, Y., Wang, J., Hu, Y., & Lei, J. (2018, November 1). A Deep Learning Approach to the Citywide Traffic Accident Risk Prediction. IEEE Xplore. https://doi.org/10.1109/ITSC.2018.8569437
62. Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Science (IJAERS), 10(5), 055–060. https://doi.org/10.22161/ijaers.105.8

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

63. Robbins, S., & van Wynsberghe, A. (2022). Our New Artificial Intelligence Infrastructure: Becoming Locked into an Unsustainable Future. Sustainability, 14(8), 4829. https://doi.org/10.3390/su14084829
64. Ross, B., Hofeditz, L., Möllmann, N. R. J., Mirbabaie, M., & Stieglitz, S. (2023). Recommendations for managing AI-driven change processes: when expectations meet reality. International Journal of Management Practice, 16(4), 407. https://doi.org/10.1504/ijmp.2023.10055048
65. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors, 23(16), 7273. https://doi.org/10.3390/s23167273
66. Samariya, D., & Thakkar, A. (2021). A Comprehensive Survey of Anomaly Detection Algorithms. Annals of Data Science. https://doi.org/10.1007/s40745-021-00362-9
67. Šegvić S., Brkić, K., Zoran Kalafatić, Vladimir Stanisavljević, Marko Ševrović, Budimir, D., & Dadić, I. (2010). A computer vision assisted geoinformation inventory for traffic infrastructure. International Conference on Intelligent Transportation Systems. https://doi.org/10.1109/itsc.2010.5624979
68. Settanni, F. (2022, April 13). Towards intelligence driven automated incident response. Webthesis.biblio.polito.it. http://webthesis.biblio.polito.it/id/eprint/22865
69. Shukla, A., & Karki, H. (2016). Application of robotics in onshore oil and gas industry—A review Part I. Robotics and Autonomous Systems, 75, 490–507. https://doi.org/10.1016/j.robot.2015.09.012
70. Şimşek, D., Kutlu, I., & Şık, B. (2023). The role and applications of artificial intelligence (AI) in disaster management. Proceedings of 3rdInternational Civil Engineering and Architecture Congress (ICEARC'23). https://doi.org/10.31462/icearc.2023.arc992
71. Singh S. K., Manjhi P. K., & Tiwari, R. S. (2021). Cloud Computing Security Using Blockchain Technology. In Book: Transforming Cybersecurity Solutions Using Blockchain (Pp.19-30). https://doi.org/10.1007/978-981-33-6858-3_2
72. Sirohi, D., Kumar, N., & Rana, P. S. (2020). Convolutional neural networks for 5G-enabled Intelligent Transportation System: A systematic review. Computer Communications, 153, 459–498. https://doi.org/10.1016/j.comcom.2020.01.058
73. Suganthi, L., Iniyan, S., & Samuel, A. A. (2015). Applications of fuzzy logic in renewable energy systems – A review. Renewable and Sustainable Energy Reviews, 48, 585–607. https://doi.org/10.1016/j.rser.2015.04.037
74. Taddeo, M., McNeish, D., Blanchard, A., & Edgar, E. (2021). Ethical Principles for Artificial Intelligence in National Defence. Philosophy & Technology, 34(4), 1707–1729. https://doi.org/10.1007/s13347-021-00482-3
75. Tatineni S. (2023). AI-Infused Threat Detection and Incident Response in Cloud Security. International Journal of Science and Research, 12(11), 998–1004. https://doi.org/10.21275/sr231113063646
76. Tomic, S., Fensel, A., & Pellegrini, T. (2010). SESAME demonstrator. In: Proceedings of the 6th International Conference on Semantic Systems. Graz, Austria, 1, 4. https://doi.org/10.1145/1839707.1839738
77. Tonhauser, M., & Jozef Ristvej. (2023). Cybersecurity Automation in Countering Cyberattacks. Transportation Research Procedia, 74, 1360–1365. https://doi.org/10.1016/j.trpro.2023.11.283
78. Umoga, J., Oluwademilade, E., Ugwuanyi, D., Jacks, S., Lottu, A., Daraojimba, D., & None Alexander Obaigbena. (2024). Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. Magna Scientia Advanced Research and Reviews, 10(1), 368–378. https://doi.org/10.30574/msarr.2024.10.1.0028
79. Veres, M., & Moussa, M. (2020). Deep Learning for Intelligent Transportation Systems: A Survey of Emerging Trends. IEEE Transactions on Intelligent Transportation Systems, 21(8), 3152–3168. https://doi.org/10.1109/tits.2019.2929020
80. Wang, C.-X., Renzo, M. D., Stanczak, S., Wang, S., & Larsson, E. G. (2020). Artificial Intelligence Enabled Wireless Networking for 5G and Beyond: Recent Advances and Future Challenges. IEEE Wireless Communications, 27(1), 16–23. https://doi.org/10.1109/mwc.001.1900292
81. Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. ICT Express, 8(3). https://doi.org/10.1016/j.icte.2022.04.007
82. Xu, Z., Lian, J., Bin, L., Hua, K., Xu, K., & Chan, H. Y. (2019). Water Price Prediction for Increasing Market Efficiency Using Random Forest Regression: A Case Study in the Western United States. Water, 11(2), 228. https://doi.org/10.3390/w11020228
83. Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Robotics Cyber security: vulnerabilities, attacks, countermeasures, and Recommendations. International Journal of Information Security, 21(21). https://doi.org/10.1007/s10207-021-00545-8
84. Yao, H., Wu, F., Ke, J., Tang, X., Jia, Y., Lu, S., Gong, P., Ye, J., & Li, Z. (2018). Deep Multi-View Spatial-Temporal Network for Taxi Demand Prediction. Proceedings of the AAAI Conference on Artificial Intelligence, 32(1). https://doi.org/10.1609/aaai.v32i1.11836
85. Yin, J., & Zhao, W. (2016). Fault diagnosis network design for vehicle on-board equipments of high-speed railway: A deep learning approach. Engineering Applications of Artificial Intelligence, 56, 250–259. https://doi.org/10.1016/j.engappai.2016.10.002
86. Zhang, X., Nguyen, H., Bui, X.-N., Anh Le, H., Nguyen-Thoi, T., Moayedi, H., & Mahesh, V. (2020). Evaluating and Predicting the Stability of Roadways in Tunnelling and Underground Space Using Artificial Neural Network-Based Particle Swarm Optimization. Tunnelling and Underground Space Technology, 103, 103517. https://doi.org/10.1016/j.tust.2020.103517

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VII, July 2024

AUTHORS BIOGRAPHY

1. **Akinkunle Akinloye** is a Highly accomplished and process-driven professional with over 13 years of experience in network security, network operations, network design and cloud computing. He is also proficient in performing threat intelligence and detection, and vulnerability assessments. He has MSc in Network Systems from University of Teessde

2. **Sunday Anwansedo** has a Masters in Electrical Enginnering with expertise in telecommunications devices and technology, including the designs and optimization of Systems and components for communication infrastructure.

3. **Oladayo Tosin Akinwande** obtained his B. Tech and M. Tech in Computer Science from Federal University of Technology, Minna, Niger State, Nigeria. He is currently a PhD Student of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria. His current research interests include artificial intelligence, explainable artificial intelligence, security and privacy issues in artificial intelligence and information and communication security. He is a member of Nigeria Computer Society (NCS).