International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure

Bright Ojo [1,*] and Chukwudi Tabitha Aghaunor [2]

[1] *Department of Operations Management, University of Arkansas, Fayetteville, AR, USA.*
[2] *Department of Cybersecurity, Robert Morris University, Pittsburgh, PA, USA.*

International Journal of Science and Research Archive, 2024, 12(02), 1716–1726

Publication history: Received on 15 June 2024; revised on 29 July 2024; accepted on 01 August 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.12.2.1401

Abstract

Cyber-security as a concept relates to the protection of critical infrastructures that are significant to the security of a nation. Because many security threats have targeted computer-based critical infrastructures, nations have considered it necessary to enhance their security to detect and predict cyber threats accurately. This paper aimed to discuss the role of artificial intelligence (AI) in increasing real-time threat detection to critical infrastructures such as water facilities and transport systems. Through the implementation and application of AI, it is easier to not only detect the threat but also counter it promptly. Thus, the paper discussed the latest AI technologies, the approaches for their use and the cases, for example, the Colonial Pipeline ransomware attack, to demonstrate AI's capabilities and limitations in this area. Other strategies such as measures and formulation of policies were also considered to ensure sound protection and improvement policies and regulations framework for cybersecurity.

Keyword: Cybersecurity; Threat Detection; Critical Infrastructure; Colonial Pipeline; Ransomware Attack; Water Systems;Transportation Networks

1. Introduction

Critical infrastructure and national security complement each other since they are both components that play a part in efficient security processes and data management. However, critical infrastructure is a term that emanated from the United States of America in the 1990s. This term has shifted over time and is in its most recent form referred to as security perspective (Alexandru et al., 2019). Technological advancement plays a key role in popularising critical infrastructure. The prevalence and complexity of cyber-attacks on critical infrastructure has become a critical concern for national security. One of the major problems of critical infrastructure security is the level of awareness of the impact of cyberattacks on critical infrastructure (Roshanaei, 2021). This indicates that while cyberattacks are aware of the possibilities to counter their attacks, they may take advantage to attempt its prediction.

However, AI-driven security solutions have become an integral part of the global security critical infrastructure due to the need to curb cyber security threats. Many industries have experienced cyber threats, and their impact has affected their businesses hence the need to prioritise AI-driven and automated cybersecurity solutions to help them with real-time threat detection (Li & Liu, 2021). These threats include spamming, phishing, malware, corporate account takeover (CATO), distributed denial of services (DDoS) attacks, ransomware, and automated teller machine (ATM) cash-out, amongst others (Mass.gov, 2024). While these attacks have been used by cyber attackers to facilitate their online activities, nations have sought different ways to counter these attacks. This has prompted the integration of AI solutions to national critical security infrastructure to help safeguard nations' economies.

* Corresponding author: Bright Ojo

1.1. Purpose of the Study

This study aims to explore AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. Cybersecurity for critical infrastructure is essential for national security due to increasing cyber threats. By synthesising relevant literature, this study will focus on high-profile cyber-attacks, such as the Colonial Pipeline ransomware attack to uncover vulnerabilities. It will discuss measures adopted by the U.S. government to enhance cybersecurity.

1.2. Research Question

What are the AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure and how can they be enhanced to reduce cyber threats for nations?

1.3. 4. Research Objectives

- To critically review existing literature on AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure.
- To identify AI technologies, implementation strategies, exploring and case studies, such as the Colonial Pipeline ransomware attack, and the civil engineering-related infrastructure such as Water Systems and Transportation Networks to illustrate the effectiveness and challenges of AI in this domain.
- To investigate the efficacy of policies and regulatory frameworks on critical infrastructure and cybersecurity.
- To recommend critical infrastructure and cybersecurity solutions for national security.

2. Literature Review

2.1. Significance of Cybersecurity in National Security

As the world progresses to a more digitised economy, nations are beginning to see the need to adopt effective cybersecurity measures to safeguard their cyberspaces. This has become paramount for advanced countries with more advanced critical infrastructure and digital economies as they face reoccurring cyber threats from attackers. Thus, cybersecurity plays a vital role in protecting national infrastructure against attacks (Kovács, 2018). According to Forescout (2024), the world's critical infrastructure experienced over 420 million cyber-attacks in 2023, with 13 attacks per second, and a 30% increase from 2022. These attacks were majorly targeted at the communication, medical, manufacturing, transportation, power, and waste industries. Financial Times (2020) also records prominent attacks on the United States's largest oil pipeline, Japan's largest port, San Francisco's light-rail system, major hospitals around the world, as well as Ukraine's critical infrastructure. According to the report, most of these attacks are usually not disclosed by the victims due to the fear of destroying stock prices and public trust. Hence, it is much easier for cyber attackers to carry out their activities since they can predict their victim's responses and the countermeasures the national security would likely implement against their operations.

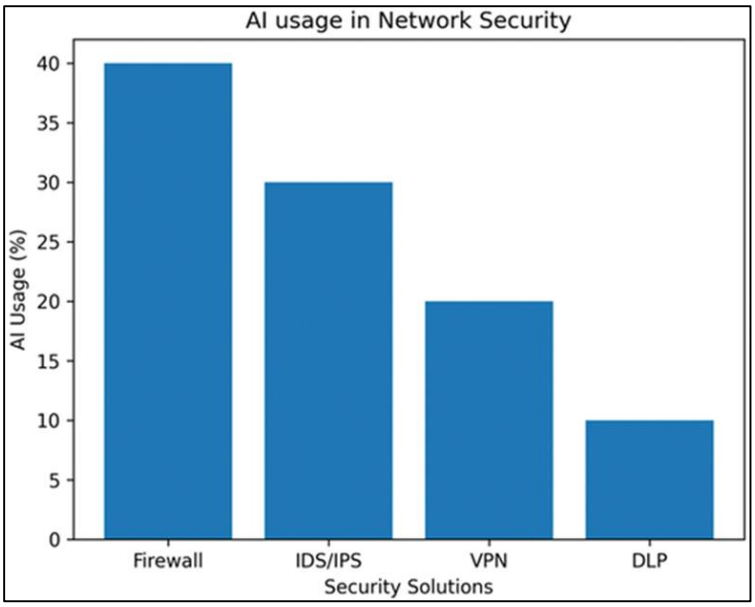

Figure 1 AI and ML Integration in Network Security (Mohamed, 2023)

Despite the numerous attacks on cyberspace, Van Noordt et al. (2023) note that national security intensifies its strategies in building a resilient critical infrastructure that captures all cyber infrastructures and networks to minimise the risks of cyber threats and ensures a safe cyberspace for public administration and their economy. These strategies involve the facilitation of Artificial intelligence (AI) research that covers various cyber activities and infrastructures. However, adopting and deploying AI within public administration may be challenging and as a result hinder various administrations from benefiting from these technologies. These challenges include ethical concerns, legal limitations, lack of expertise, lack of quality data, and lack of inter-organisational collaboration, amongst others (Van Noordt et al., 2023).

2.2. Case Studies/Areas to Focus On

2.2.1. Colonial Pipeline Ransomware Attack

The Colonial Pipeline ransomware attack of May 2021 revealed major shortcomings in the cybersecurity protection of critical industries in the United States. The hackers got into the system through a VPN that lacked two-factor authentication, showing the dangers of weak protection practices. The event disrupted 45% of the East Coast's fuel supply, of which the effects of cyber attacks on national infrastructure are well exemplified (Greubel et al., 2023). AI could perhaps help avert such occurrences as it integrates threat detection and response mechanisms efficiently. For example, AI systems can be designed to detect intricate features of network traffic and alert risks of security breaches online (Binhammad et al., 2024). However, the predictive modelling that AI offers can reveal loopholes that might be exploited in the future hence enabling organisations to resolve them. As a result, AI can detect compromised credentials and other suspicious activity related to ransomware through the use of machine learning algorithms, hence significantly decreasing response time (Sarker, 2022).

Thus, in response to such threats, the US government has upped attempts to strengthen its cybersecurity measures, including the use of artificial intelligence AI. Real-time monitoring and analysis of large volumes of data are crucial in the identification of potential threats and vulnerabilities as a result, AI can augment the threat identification and management procedures (Jawaid, 2023). This is required to ensure that National security predicts an attack before it can significantly affect victims. The Colonial Pipeline event still holds a lot of lessons on using cybersecurity to protect critical infrastructure and the need to improve defence strategies to overcome emerging threats (Greubel et al., 2023).

2.2.2. Water Systems and Transportation Networks

In the civil engineering field, water systems and transportation networks need to be protected from cyber-attacks as they threaten public safety and service reliability. McMillan & Varga (2022) note that water systems remain highly prone to cyber-attacks since most of them are fitted with obsolete systems and have inadequate security monitoring. For example, due to a lack of software updates over time, the existing computer systems lack security measures, such as encryption for messages and secure communication. There are potential protective measures that centre AI solutions and serve to counter these vulnerabilities. AI can help analyse water quality and supply systems by identifying issues likely to cause failure or contamination, rectifying them before they happen and designing the supply system to ensure that consumers always have a constant flow of water (Fu et al., 2022).

In transportation networks, AI can improve traffic management systems by recognising possible cyber threats and preventing them within networks. For instance, using a cloud interface, AI can examine traffic patterns and sensors' data to recognise anomalies that point to a cyber attack so that countermeasures can be taken (Nasim et al., 2023). In addition, through the evaluation of the data collected from different sensors, it becomes possible to use AI to predict equipment failure thus enhancing the reliability of machining systems while minimising the extent of downtime. Nevertheless, the introduction of AI raises some concerns about civil infrastructures as well. Some drawbacks include doubts about AI's ability to withstand potent cyber threats and worries that AI can only be protective if it is integrated correctly (Bharadiya, 2023). Moreover, sometimes the expense of implementing AI technologies is high and there may be a requirement for a skilled workforce to govern such systems, which may act as hurdles for the government. Despite these challenges, Jada and Mayayise (2023) indicate that AI has the potential to transform how infrastructure security is conducted and thus remains an integral part of engineering procedures in the contemporary world. By addressing these critical issues, AI can also have a groundbreaking impact on defending crucial services against new forms of cyber threats.

2.3. Importance of Cybersecurity for Critical Infrastructure

Critical infrastructures are valued assets for government and administrative functions, economic welfare, public safety, and the national security of any country. These infrastructures broadly consist of physical, and cyber elements including financial services, communication networks, transportation systems, and the public service sector (Roshanaei, 2021).

Before the 21st century, critical infrastructure was more of a physical activity where different sectors and national security agencies collaborated to improvise various techniques of countering all sorts of threats affecting them. However, with the advancement of technology and the prevalent cyber threats, critical infrastructure has progressed to include cyber infrastructures. The 21st threat thus experiences cyber threats that can endanger any effective critical infrastructure leaving the society and the nation's economy vulnerable. As such, cybersecurity is crucial as it can bluster critical infrastructure, maintain cyber integrity, improve innovation and national security, and boost economic growth (Alexandru et al., 2019).

2.4. Role of AI in Enhancing Real-Time Threat Detection

AI is an effective tool for threat detection owing to its capability to scrutinise real-time data. According to Binhammad et al. (2024), the traditional method of data detection relying on predefined instructions is slow and inefficient. Thus, it allows hackers to carry out their operations before detecting them. On the other hand, AI can learn new data, improve anomaly detection, identify trends and patterns, and quickly adapt to new threats that are invisible to analysts. Binhammad et al (2024) focus on AI on information security and the advantages and disadvantages of AI. The researchers explore models that further enhance or cause the degrading of infrastructure functions for this exercise. This involves the creation of cybersecurity software and AI-immune plans that can prevent these weaknesses. The report shows that AI improves accurate real-time threat recognition and security preventive work, and increases the security operations effectiveness. On this note, it is important to note weaknesses of AI including security vulnerabilities, ethical concerns, poor interpretability, and data bias.

Therefore, based on these limitations, nations and agencies who wish to implement AI for threat detection in real-time need to be informed of these flaws. Cyber threats at times may be intricate making it difficult for AI to identify them hence the need for professionals to train or opt for early versions of the AI algorithms for the new threats. This is very important for the establishment of an efficient and strong cyber security network managing vulnerability and forming a fundamental defence mechanism against cyber threats (Kaur et al., 2023).

2.5. Implementation Strategies and Technologies

Currently, there is a dynamic nature of cybersecurity due to the incorporation of AI and ML in the existing and emerging cybersecurity versions. Similar to AI, ML has transformed the cybersecurity system in the best way possible. As a result, it is possible to emphasise that the inclusion of these technologies into the cybersecurity frameworks can enhance real-time detection. AI and ML are also embedded in the cybersecurity analysis phase, which can similarly compare the same data from the different administrations or other organisations' digital systems to detect threats that conventional methods cannot discern. For this, the ML models use intricate algorithms on such data with enhanced focus and speed than a human being could manage. As noted in the article by Roshanaei et al. (2024), innovative advancements in the field of ML and AI have bolstered the cybersecurity system. Such trends as neural networks, deep learning models, and reinforcement learning are among the elements of the IoT which assist in autonomous response systems, and anomalous dependencies investigation.

Neural networks and deep learning models are recent trends in the AI landscape for mimicking human and animal brains. These are efficient in categorising complicated abnormalities and patterns from databases hence improving on the quick identification of threats. On the other hand, reinforcement learning however utilises dynamic inputs to inform AI systems about updated data and information while familiarising them to new threats in real-time. Recently, organisations are beginning to adopt quantum computing as the new method of encrypting data and strengthening the cybersecurity system. Due to the ineffectiveness of traditional encryption methods against sophisticated cyberattacks, quantum computing provides unmatched computing proficiencies for improving cybersecurity. This technology has transformed how sensitive data are protected by integrating AI-quantum-based machine learning modules and quantum-resistant encryption algorithms to safeguard critical infrastructures (Agrawal, 2024).

2.6. Policy and Regulatory Frameworks

Cyberthreats cut across nations, countries, and organisations escalating their impact on vulnerable victims and organisations. Nations have different policies and regulatory frameworks for cybersecurity. Some nations' cybersecurity policies make it easier for cybercriminals to perpetrate their activities with little or no clue for governments to track down these criminals (Mishra et al., 2022). As such, thorough cybersecurity policies and regulatory frameworks are required for governments to implement while tracking down cyber threats. Mishra et al. (2022) investigate a regulatory framework for protecting critical infrastructures against cyber threats in the European Union (EU). The researchers explore the coverage and effectiveness of the CI protection policies and regulations for cybersecurity, pointing out that there is a vast range of measures that remain constant in development.

The EU for example has been active since 2004 with guidelines such as the European Programme for Critical Infrastructure Protection (EPCIP) and the NIS Directive. They primarily address specific risks and promote higher levels of defence against cyber risks (Pursiainen & Kytömaa, 2022). However, this has inherent weaknesses in terms of its reliance on a sector approach, one which at the time focused only on the energy and transport sectors. This implies that vital sectors like health, water and sanitation, and financial services have been left underdressed. This is a major drawback given the fact that critical infrastructures are interdependent and hence, vulnerable to ever-changing cyber threats.

Extending to the various sectors of the nations, it is clear that some sectors also have these regulatory deficits as identified by Mishra et al (2022). For example, water supply and transport and logistics networks that are considered to be critical infrastructures have poor technological infrastructure as well as inadequate security features. Kaspersky (2021) shows that AI-based solutions may improve the security of such systems by analysing the situation in real-time and predicting possible risks. Likewise, the financial sector, which depends on IT structures for its primary operations, needs strong security systems to protect against such cyber threats. Studies show that the addition of AI and machine learning can enhance threat detection and protection in this industry by up to 80% (Buczak & Guven, 2016). Thus, the existing regulation models and frameworks do give some protection to critical infrastructures, and there is a need to broaden the approaches and include new and more effective means such as AI.

3. Research Methodology

3.1. Research Design

This study adopted a mixed-method approach incorporating quantitative and qualitative research techniques (Hands, 2022). To achieve the research aim, the quantitative technique consisted of a survey distributed to Cybersecurity Professionals including Cybersecurity Consultants, Security Analysts and Engineers, and Data Scientists and Machine Learning Engineers. These respondents were required to give their answers through an online questionnaire prepared with predetermined questions and sent through email.

In contrast, the qualitative approach entailed the critical analysis of peer-reviewed journals, as well as industry and government reports to determine the existing AI technologies, the way and manner that they are deployed, along with actual case studies exemplified by the use of AI in the Colonial Pipeline ransomware attack. Further, the review analysed the effectiveness of policies and regulation standards for the protection of the core infrastructure and cybersecurity along with suggesting measures for core infrastructures and cybersecurity for National security.

3.2. Data Analysis

Quantitative data analysis involved the use of descriptive statistics, which calculated, described, and summarised data logically collected from respondents (Kaur et al., 2018). In the same regard, thematic analysis is involved in qualitative data analysis to examine trends as well as patterns recurrent in the analysed studies and in addition, to discern resemblance and disparity between them (Naeem et al., 2023).

3.3. Ethical Considerations

Ethical considerations were observed to safeguard the interests of the respondents as well as the researcher. This includes explaining the purpose of the study and the need for voluntary participation to the respondents before administering the survey (Cacciattolo, 2015). Hence, the researcher also maintained accountability and credibility while conducting the research.

4. Result

The key findings from the mixed-methods evaluation of AI-driven cybersecurity solutions for real-time threat detection in critical areas are presented below. Peer-reviewed articles explored in this study have defined critical infrastructure and cybersecurity. They also discussed the relationship between critical infrastructure and national security, uncovering the cybersecurity threats and AI-driven solutions for real-time detection.

4.1. The Impact of AI and ML Solutions on Cybersecurity Threats

Cyber attacks have become a major threat to national security with a historical record (see Appendix 1). These attacks come in different forms leaving the State and national infrastructure vulnerable. Among these attacks are IoT attacks,

ransomware attacks, malware attacks, encrypted threats, intrusion attempts, and crypto-jacking attacks (Roshanaei et al., 2024).

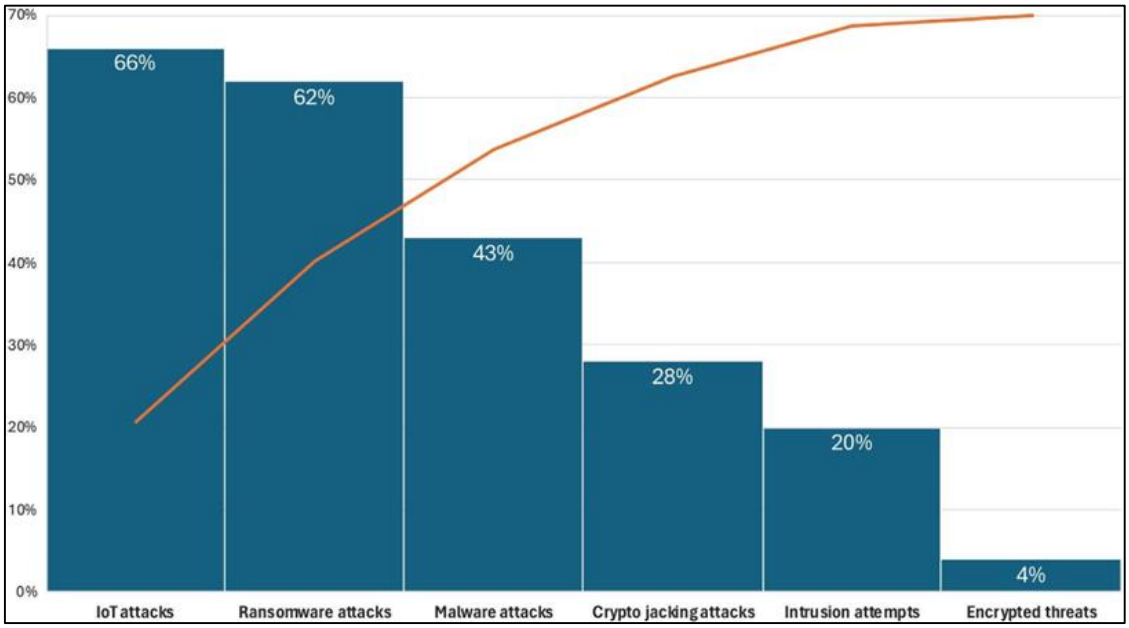

Figure 2 Historical Progress of Cyber Threats and Responses (Roshanaei et al., 2024)

Moreover, the integration of AI and ML models is considered a significant force in cybersecurity since it improves protection against constantly evolving threats. These technologies assist in threat identification in real-time, which shows the applicability of AI in processing large data in small portions and evaluating the risks and threats (Bresniker et al., 2019). For example, AI can monitor certain peaks of traffic or certain deviations of actions of users that are not normal, and then signal a breach attempt. Moreover, the existence and application of AI algorithms will be to quickly identify anything in the form of a threat or an attack on the systems and networks because of the different traffic flows or behaviour that might depict hacking or other instances of security breaches (Roshanaei et al., 2024). This provides an adequate argument for the employment of AI and ML as an ideal resolution to real-time threat identification and national security.

Further, unlike traditional methods, the ML models incorporate large historical data to perform highly sophisticated pattern recognition. This enables one to identify any pattern that is associated with different types of threats such as advanced phishing scams and even other types of threats which are insider threats and may not easily be spotted by traditional tools (Taye, 2023). Moreover, these solutions (AI and ML) could have helped the US national security to detect the Colonial Pipeline ransomware attack on their critical industries in the United States (Greubel et al., 2023). While these solutions prove effective in different organisations, they are not without challenges.

4.2. AI-driven Challenges for Cybersecurity Threats

Integrating AI and ML in cybersecurity frameworks are indeed solutions that bring about radical improvements but at the same time come with several issues (see Appendix 2). AI and ML models are easily under threats, where the input data can be manipulated to make the threat-detection system fail, affecting users' trust. Additionally, these models depend on the quality and amount of training data, hence poor and minimal data may lead to ineffective as well as biased models raising issues of data ownership (Roshanaei et al., 2024). These challenges demonstrate that while national security could benefit from AI-driven solutions, it still needs to be aware of the possible pitfalls, hence intensifying its strategies towards safeguarding the nation's cyberspace.

5. Discussion

Cyber threats have been researched and recorded as persisting threats to nations' critical infrastructures. This study covered the discourse on the Colonial Pipeline ransomware attack, water systems and transportation networks, and major shortcomings of the cybersecurity protection of critical industries in the United States. AI-driven solutions are necessary to tackle the evolving cyber threats to national security. Employing a systematic review, Daniel and Victor

(2024) evaluated the cybersecurity landscape for critical infrastructure, concentrating on evolving trends, contemporary issues, and prospects. This aligns with the present research on AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. The main focus of the review is to discuss the new trends and focus areas in cybersecurity, such as the use of artificial intelligence and machine learning to detect threats, protection of the IoT, blockchain solutions, and innovations in the protection of cloud computing systems. Future risks and threats, such as advanced persistent threats, or risks connected to quantum computing breakthroughs, are investigated to identify possible weaknesses.

Furthermore, ML models were found to be key tools for detecting cyber threats. The severity of cyber threats impacting nations has prompted the urgency in developing a more resilient critical infrastructure for stable and crisis-prone critical infrastructures. While the Colonial Pipeline ransomware attack exposed major limitations in the US critical infrastructure and cybersecurity, national security required intensified cybersecurity to safeguard cyberspace. This reinforces the importance of the integration of AI and ML to strengthen their security protocols. ML helps in obtaining and processing data, extracting relevant features, and classifying predictions.

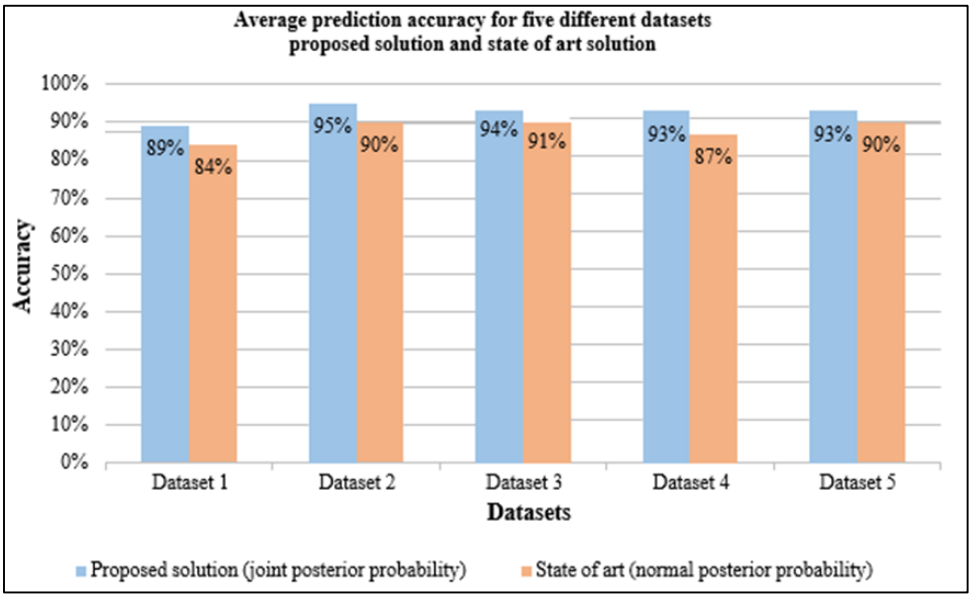

Figure 3 Prediction Accuracy for Five Datasets Proposed for Cybersecurity Solution

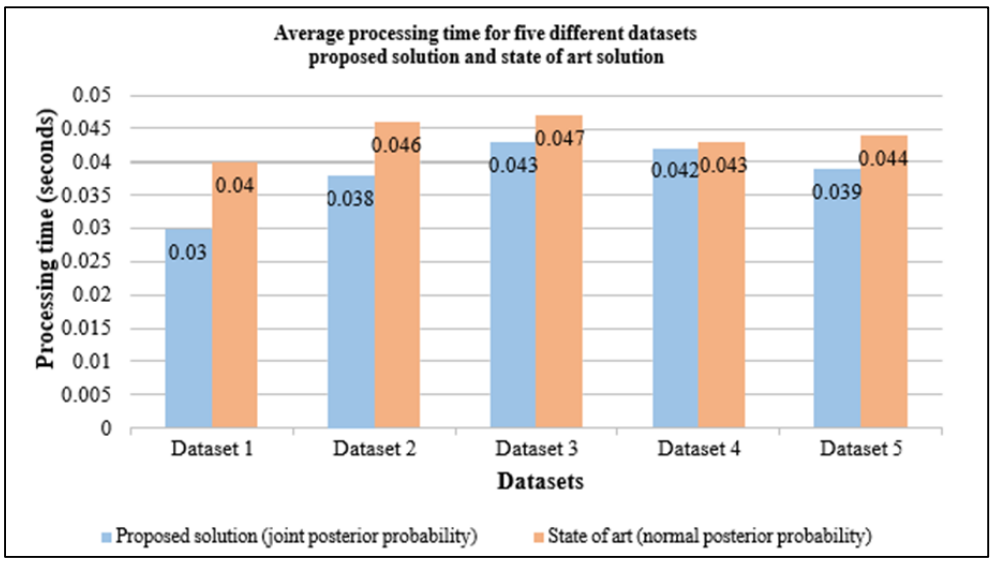

Figure 4 Processing times for Five Datasets Proposed for Cybersecurity solutions

Moreover, the study utilised a quantitative method to examine five datasets consisting of 328,814 threat samples which were utilised to determine the accuracy result and processing time for the proposed solution (Sentuna et al., 2020). It reveals that the solution is effective in predicting and processing threats rapidly in different scenarios from 92–96% and reduces the average processing time from 0.043 to 0.028 compared with the traditional detection methods.

Five datasets had their average processing times examined. Blue outlines show what the suggested solution's values are. Alternatively, the range outlines show the state-of-the-art solution values. The first two columns in the above graph show how many seconds on average Dataset 1 takes to complete the operation. Columns two and three show Dataset 2 average processing time. The second and third columns show the chosen average processing time for Dataset 3. The average amount of time needed to analyse Dataset 4 is shown in the last two columns. The average amount of time needed to analyse dataset 5 is shown in the fifth and second columns.

For the first dataset, which depends on true positive and true negative outcomes, the mean has been provided in terms of percentage. The true graphical depiction of this has blue lines, which show the solution values of the suggested solution. As for solution 2, it should be noted that the orange colour indicates the values of the state of the art. From the given dataset, the real positive mean accuracy value is depicted in the first two columns. Few epochs are expected by the suggested method and this implies that the processing time values will decrease if the size of the dataset has gone up. The second and third columns of the code demonstrate the mean value of the true negative that attains the best accuracy. The ML framework below illustrates the detection and prediction of cyber threats.

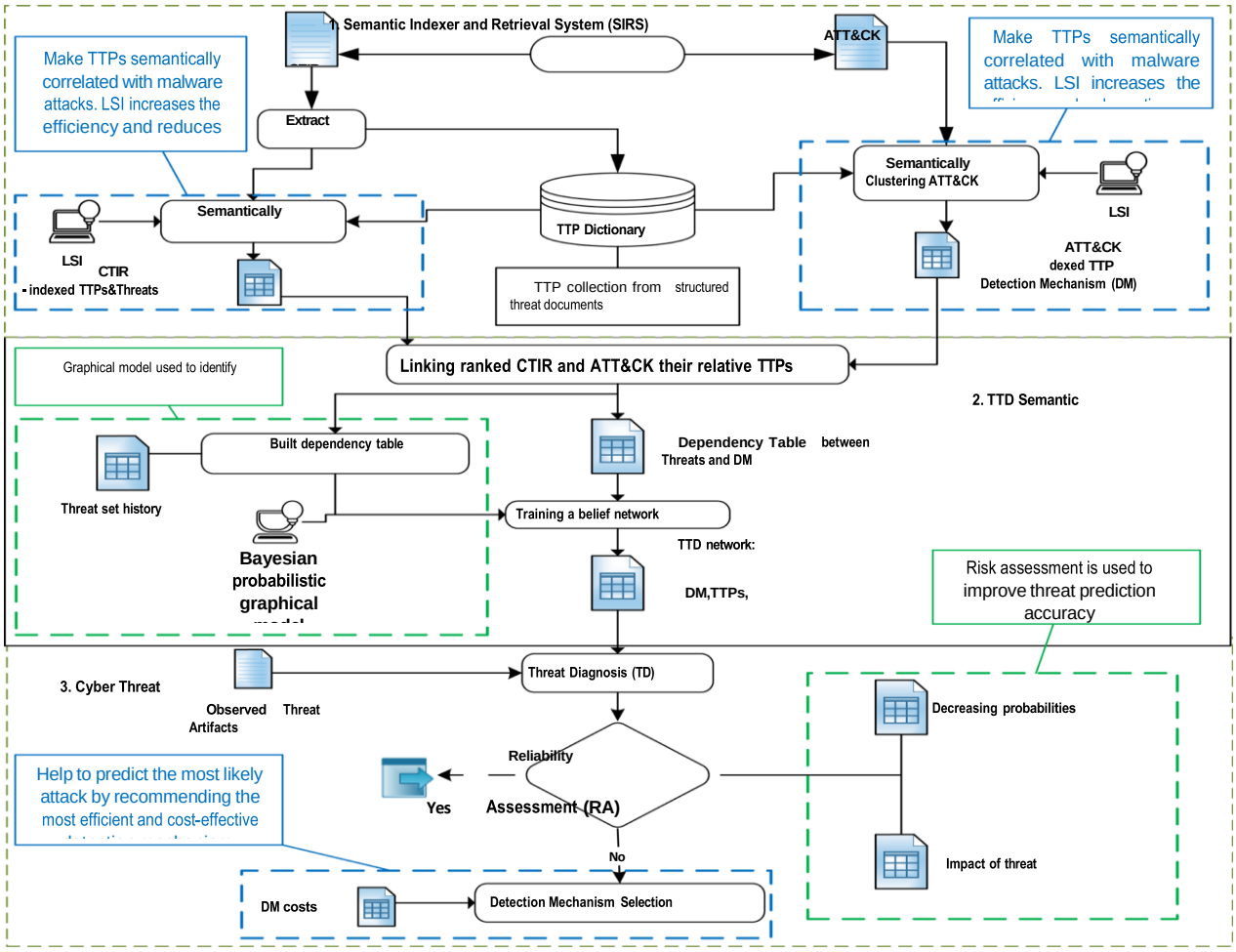

Figure 5 ML Bayesian Probabilistic Graphical Algorithm (Sentuna et al., 2020)

Utilising an ML method known as Bayesian probabilistic graphical algorithm, the proposed framework augments AI cybersecurity to improve its use in threat detection within essential facilities of the United States. In this framework, tactics, techniques, and procedures (TTPs) are extracted by the system from well-defined threat reports and form the TTP dictionary within the system. This makes TTPs semantically related to malware attacks by utilising Latent Semantic Indexing (LSI) for enhanced detection. A Bayesian model predicts threat occurrence based on the historical data

collected where it is also possible to calculate threat probability and its dependency. The framework is adaptive in dealing with risk and categorises risks based on threat impact and reliability, reduces wrong decisions, and is effective in the utilisation of resources. The goal of this approach is to ensure that threats are detected and dealt with appropriately and effectively.

5.1. Cross-Sectoral Findings and Policy Implications

The research explores various studies on cybersecurity, cyber threats and critical infrastructure. Having considered multiple threats to nations' infrastructure including the Colonial Pipeline ransomware attack on the US infrastructure, it is necessary to come up with effective solutions to curb cyberthreats impacting the nation's economy. While recognising the need for an effective solution for cyber threats, it is imperative to consider the challenges associated with this effort including a lack of AI and ML expertise and a lack of policy and regulatory frameworks guiding different nations.

Hence, to develop an effective policy, the US needs to review their formal cybersecurity policies, ensuring that the most recent AI algorithms are captured. This would help the AI system learn and predict future threats based on predetermined data. Moreover, collaborating with different countries would benefit the countries' national security as they can assess useful data that may help track down cyber threats.

6. Conclusion

This study has scrutinised AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. The research utilises a mixed-method research technique to examine the Colonial Pipeline ransomware attack. It emphasises how AI can prevent similar incidents. It also discusses water systems and transportation networks focusing on civil engineering-related infrastructure, and highlighting vulnerabilities and AI-driven solutions. The study found that cybersecurity is crucial for critical infrastructure. Considering the case study on the colonial pipeline ransomware attack on the US infrastructure, it outlines AI-driven solutions such as the integration of AI and ML models to enhance real-time threat detection and prediction for national security. Moreover, ML models have been proven to be effective in different organisations including information technology, health, transport, water, and sanitation. This shows that it would be relevant for the US national security. Additionally, implementing an effective policy and regulatory framework would help the US expand its security networks to accommodate the evolving AI trends.

Recommendations

Based on the literature review, the study provides various recommendations to improve national cybersecurity infrastructure using AI-driven solutions:

- **Leverage AI and ML models:** National security should leverage AI and ML methods to strengthen the cybersecurity infrastructure.
- **Implement Continuous Learning and Adaptation:** Ensure that AI systems are trained to learn new data for more effective real-time threat detection and prediction.
- **Collaboration and Knowledge Sharing:** Collaborate and share knowledge and best practices, between governments, academic institutions, industries, and countries to improve threat detection.
- **Prioritise Data Privacy and Security**: Implement robust data privacy and security protocols to ensure that sensitive data are protected and utilised in training AI models.
- **Improve policies and Regulatory Frameworks:** Review and amend old policies while creating a robust regulatory and ethical framework for decision-making on cybersecurity.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Agrawal, S. (2024). Harnessing Quantum Cryptography and Artificial intelligence for next - gen payment Security: A Comprehensive analysis of threats and countermeasures in distributed ledger environments. International Journal of Science and Research, 13(3), 682–687. https://doi.org/10.21275/sr24309103650

[2] Alexandru, A., Vevera, V., & Ciupercă, E. M. (2019). National security and critical infrastructure protection. International Conference Knowledge Based Organization, 25(1), 8–13. https://doi.org/10.2478/kbo-2019-0001

[3] Bharadiya, J. (2023). Artificial intelligence in Transportation Systems A critical review. American Journal of Computing and Engineering, 6(1), 34–45. https://doi.org/10.47672/ajce.1487

[4] Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The role of AI in Cyber Security: Safeguarding Digital identity. Journal of Information Security, 15(02), 245–278. https://doi.org/10.4236/jis.2024.152015

[5] Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2019). Grand challenge: Applying artificial intelligence and machine learning to cybersecurity. Computer, 52(12), 45–52. https://doi.org/10.1109/mc.2019.2942584

[6] Cacciattolo, M. (2015). Ethical considerations in research. In SensePublishers eBooks (pp. 61–79). https://doi.org/10.1007/978-94-6300-112-0_4

[7] Daniel, N. S. A., & Victor, N. S. 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

[8] Financial Times. (2020). How critical infrastructure across the globe is targeted by cyber attacks. Financial Times - Partner Content by Yubico. https://www.ft.com/partnercontent/yubico/how-critical-infrastructure-across-the-globe-is-targeted-by-cyber-attacks.html

[9] Forescout. (2024). At 13 attacks per second, critical infrastructure is under siege. https://www.forescout.com/press-releases/2023-threat-roundup/

[10] Fu, G., Jin, Y., Sun, S., Yuan, Z., & Butler, D. (2022). The role of deep learning in urban water management: A critical review. Water Research, 223, 118973. https://doi.org/10.1016/j.watres.2022.118973

[11] Greubel, A., Andres, D., & Hennecke, M. (2023). Analysing Reporting on Ransomware Incidents: A case study. Social Sciences, 12(5), 265. https://doi.org/10.3390/socsci12050265

[12] Hands, A. S. (2022). Integrating quantitative and qualitative data in mixed methods research: An illustration. Canadian Journal of Information and Library Science/the Canadian Journal of Information and Library Science, 45(1), 1–20. https://doi.org/10.5206/cjilsrcsib.v45i1.10645

[13] 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. https://doi.org/10.1016/j.dim.2023.100063

[14] Jawaid, S. A. (2023). Artificial Intelligence with Respect to Cyber Security. Deleted Journal, 1(2), 96–102. https://doi.org/10.18178/jaai.2023.1.2.96-102

[15] Kaur, P., Stoltzfus, J., & Yellapu, V. (2018). Descriptive statistics. International Journal of Academic Medicine, 4(1), 60. https://doi.org/10.4103/ijam.ijam_7_18

[16] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[17] Kovács, L. (2018). National cyber security as the cornerstone of national security. Revista Academiei Forţelor Terestre, 23(2), 113–120. https://doi.org/10.2478/raft-2018-0013

[18] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

[19] Mass.gov. (2024). Know the types of cyber threats. https://www.mass.gov/info-details/know-the-types-of-cyber-threats

[20] McMillan, L., & Varga, L. (2022). A review of the use of artificial intelligence methods in infrastructure systems. Engineering Applications of Artificial Intelligence, 116, 105472. https://doi.org/10.1016/j.engappai.2022.105472

[21] Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: Evidence from seven nations. Computers & Security, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820

[22] 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

[23] Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A Step-by-Step process of thematic analysis to develop a conceptual model in qualitative research. International Journal of Qualitative Methods, 22. https://doi.org/10.1177/16094069231205789

[24] Nasim, S. F., Qaiser, A., Abrar, N., & Kulsoom, U. (2023). Implementation of AI in traffic Management: need, current techniques and challenges. Pakistan Journal of Scientific Research, 3(1), 20–25. https://doi.org/10.57041/pjosr.v3i1.942

[25] Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? Sustainable and Resilient Infrastructure, 8(sup1), 85–101. https://doi.org/10.1080/23789689.2022.2128562

[26] Roshanaei, M. (2021). Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. Journal of Computer and Communications, 09(08), 80–102. https://doi.org/10.4236/jcc.2021.98006

[27] Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024). Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions. Journal of Information Security, 15(03), 320–339. https://doi.org/10.4236/jis.2024.153019

[28] Sarker, I. H. (2022). AI-Based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN Computer Science/SN Computer Science, 3(2). https://doi.org/10.1007/s42979-022-01043-x

[29] Sentuna, A., Alsadoon, A., Prasad, P. W. C., Saadeh, M., & Alsadoon, O. H. (2020). A novel enhanced Naïve Bayes Posterior Probability (ENBPP) using machine learning: Cyber Threat Analysis. Neural Processing Letters/Neural Processing Letters, 53(1), 177–209. https://doi.org/10.1007/s11063-020-10381-x

[30] Taye, M. M. (2023). Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions. Computers, 12(5), 91. https://doi.org/10.3390/computers12050091

[31] Van Noordt, C., Medaglia, R., & Tangi, L. (2023). Policy initiatives for Artificial Intelligence-enabled government: An analysis of national strategies in Europe. Public Policy and Administration. https://doi.org/10.1177/09520767231198411

Appendices

Appendix 1: Cyber Attack Trends (Roshanaei et al., 2024)

Cyber Attack Trends	Percentage	Number of Attacks
Malware attacks	43%	5.6 billion
Encrypted threats	4%	3.8 million
Intrusion attempts	20%	4.8 trillion
Crypto jacking attacks	28%	304.6 million
Ransomware attacks	62%	304.6 million
IoT attacks	66%	56.9 million

Appendix 2 AI-driven Challenges for Cybersecurity Threats (Roshanaei et al., 2024)

Challenge	Description	Impact Level
Data Quality and Availability	Dependency on a high-quality, large database	High
Model Bias and Fairness	Risks of biassed AI outcomes due to non-representative data	Medium
Adversarial AI Attacks	Threats from malicious uses of AI against AI system	High
Integration and Operational Costs	Costs associated with integrating and maintaining AI/ML	Medium