Asian Journal of Research in Computer Science

Volume 17, Issue 10, Page 1-11, 2024; Article no.AJRCOS.124252
ISSN: 2581-8260

Leveraging AI and Machine Learning for the Protection of Critical National Infrastructure

Oluwatobiloba Okusi [a*]

[a] *Bristol Waste Company, Albert Road, Bristol BS2 0XS, UK.*

Author's contribution

The sole author designed, analysed, interpreted and prepared the manuscript.

Article Information

DOI: https://doi.org/10.9734/ajrcos/2024/v17i10505

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/124252

Review Article

Received: 21/07/2024
Accepted: 23/09/2024
Published: 27/09/2024

ABSTRACT

No nation can exist or survive without critical infrastructure (CI), which is why a nation's growth, development, welling, standard of living, possessions, and even governance are weighed by the kind of CI obtained therein. There are growing concerns about the need and how to protect CI from cyber threats in the 21st century era of digitalization. This descriptive survey research aims at showing how artificial intelligence (AI) and machine learning (ML) can be leveraged for the protection of critical national infrastructure (CNI). The study relies on secondary data, which are subjected to thematic systematic review. Interpretive and descriptive analytic techniques are used. The analysis shows that leveraging AI and ML for the protection can yield huge results, as they optimize detection of and response to threats, facilitate efficient physical maintenance, optimally evaluate and manage risks, increase awareness, and simulate and train human employees in the CNI sector. The study concludes that these cutting edge technologies have more capacities and opportunities for the protection of CNI from cyber threats than other non-technological and less

**Corresponding author: E-mail: tobi.okusi@bristolwastecompany.co.uk;*

Cite as: *Okusi, Oluwatobiloba. 2024. "Leveraging AI and Machine Learning for the Protection of Critical National Infrastructure". Asian Journal of Research in Computer Science 17 (10):1-11. https://doi.org/10.9734/ajrcos/2024/v17i10505.*

advanced technological mechanisms. It calls on stakeholders, especially national governments and authorities of the organizations involved in CNI, to make concerted efforts to surmount the challenges of AI and ML adoption and ensure significant protection of CNI across nations of the globe. Doing so would pave way for extensive practical usage of AI and ML for the protection of CNI.

Keywords: AI; machine learning; leveraging; protection; critical national infrastructure.

1. INTRODUCTION

The social and economic infrastructures of a country are critical to it. Being overwhelmingly relevant and critical to every nation and its citizens and leaders, it is important to protect the critical national infrastructure (CNI) of a nation. Infrastructure refers to the essential physical and organizational structures and facilities (e.g. buildings, roads, schools, power line supplies, water supply, transportation, telecommunications, and healthcare) needed by countries and enterprises for different operations [1,2]. These facilitate and impact positively on trade and commerce, transportation, economic growth, and the standard or quality of life of a particular nation, region or organization.

The growing cyber security threats to CNI pose serious challenges to operations in various spheres and serious risks to national security among nations (Yigit et al., 2018). There are different ways of protecting the CNI of every nation. Different cutting edge technologies can serve the purpose of protecting a nation's CNI. Emerging technologies are affirmed to be viable mechanisms for meeting the infrastructural development of the US and other nations of the world [3,4]. Extant studies confirm that AI technologies have problem-solving potentials in structural spheres, such as the construction industry [5-10]. Thus, there is the dire need to deploy emerging technologies for the protection of CNI in all nations of the world. For this study, those to deploy for the protection of CNI are artificial intelligence (AI) and machine learning (ML) models. The following diagram shows categories of critical infrastructure, its components and the directions of threats and protection.

The foregoing points are given credence by Mustyala's [11] which indicates that it is in the effort to mitigate the emerging cyber security threats to CI that fintech companies now increasingly integrate AI and ML models into the security of their infrastructure. This study rises to advocate the leveraging of AI and ML for the protection of CNI across nations, stressing that doing so would allow for the harnessing of problem-solving potentials of AI technologies in the CNI sector.

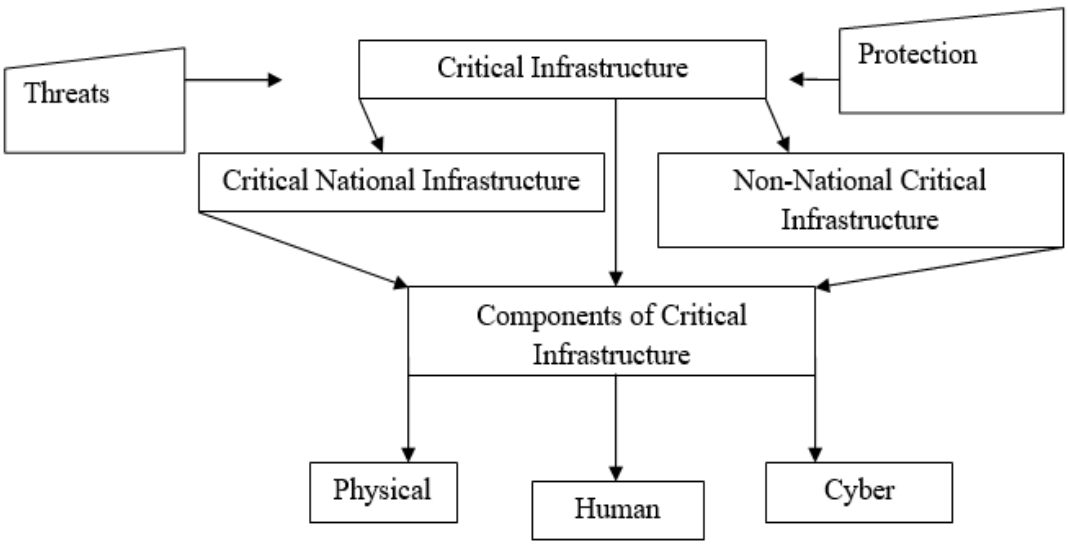

Fig. 1. Representation of infrastructure
Source: Author, 2024

1.1 Aim and Objectives

The purpose of this study is to explore the critical role of AI and ML play in the protection of critical national infrastructure (CNI). The specific objectives are to:

(i) Propose the leveraging of AI and ML for the protection of CNI.
(ii) Determine the extent to which AI and ML can help in protecting CNI.
(iii) Show how AI and ML can be leveraged for the protection of CNI.

1.2 Research Question

The study is guided by the following research questions:

(i) Should AI and ML be leveraged for the protection of CNI?
(ii) To what extent can AI and ML help in the protection of CNI?
(iii) How can AI and ML be leveraged for the Protection of CNI?

1.3 Statement of Problem

The disruption of CNI can adversely affect standard of life, public safety, economic growth,and political stability as well as pose serious risks to the national affairs and well-being of a nation. To avoid disruption, there is need to leverage AI and ML for the protection of CNI. There are many threats to CNI, which include natural disasters, cyberattacks, terrorism, vandalism, and lack of maintenance. A typical example is the Colonial Pipeline ransomware attack in the US in 2021, which led to fuel shortage and economic consequences [12]. The Danish power grid attack is another ample example. The attack by the Russian GRU 22 Danish grid operators in May 2023 destabilized grid stability [13].

Climate change and natural disasters like flood also pose serious threats to CNI. Natural disasters like hurricanes, wildfires and flood pose serious threats to lives and property, and disrupt the services as well as gains of CNI [14]. Insider threats to CNI, which include human errors and ill-acts of disgruntled employees, also affect CNI. Therefore, this study considers AI and ML as strategic technology-based mechanisms for tackling the threats to CNI. These mechanisms, the study argues, are proactive, efficacious, result-oriented, problem-solving, tech-savvy, and functionally multifarious. The major problem is that attitudinal factors continue to work against the (extent of) adoption of AI and ML where supposed. The unwillingness of members of political and elitist classes to do the needful has a bearing to attitudinal factors. These factors also pose threats to CNI.

Again, the increasing threats to critical national infrastructure ought to be combated by deploying technological methods of protecting them. This study hopes that leveraging AI and ML for the protection of CNI would yield more results and solve a whole lot of the current widespread threats to CNI across the globe. It argues that the problem-solving capabilities of AI and ML can be realized in the protection of CNI.

2. METHODOLOGY

This study relied on secondary data alongside experiential learning, field-based experiences and observations of the researcher. Closely related literatures were obtained from the internet. In searching for the data, the focus was on repositories, databases and websites. These include Google Scholar, ResearchGate, Academia.edu, Semantic Scholar, and the websites of refereed journals that are ranked by the aforementioned repositories and others. The data were subjected to descriptive and qualitative synthesis, interpretation, and analysis. With the aforementioned and the nature of the study, thematic systematic was adopted.

That is, the review focuses on the thematic concerns (findings), leaving out other elements like titles and methodologies of the sourced literatures. The exclusion and inclusion criteria of systematic review were employed. Articles considered unsatisfactory in terms of quality and not closely related to the thematic concerns of the present study were excluded. The opposites were included and relied on. On the basis of relatedness, some literatures are cited more than the others. The citations do not imply the use of the ideas of the cited authors. Rather, such authors are cited for scholarly backing. That is, while expressing views on the thematic concerns, the present study made references to related studies containing related views. The analytic techniques employed include objectivity,

criticality, logical interpretation and systemic description.

3. AI AND ML AND THEIR FUNCTIONS IN PROTECTING CNI

Here, the study shows evidence, based on descriptive survey, for the functions of AI and ML in the protection of CNI. Accordingly, Mustyala [11] shows that the capability of AI and ML to quell cyber security threats to critical infrastructure (CI) accounts for why fintech companies are increasing integrating AI and ML into their CI management and security systems. The following Table 1 presents the popular AI technologies that are capable of addressing the cyber security issues affecting CNI across nations.

Table1. Some popular AI technologies

AI Technologies	Citations
Machine Learning	Akinola [3]
Deep learning	Akinola et al.[4]
Computer Vision	Kodete et al. [15]
Reinforcement Learning	Okusi [16]
Robotic Process	Pasupuleti et al. [17]
Automation	Thapaliya and
Natural Language	Bokani [18]
Processing	Alsakka et al. [19]
Automated Machinery	Ivanova et al. [7]
Systems	Regona et al. [8]
Faster R-CNN	Wusu et al. [20]
Digital Image Analysis	Vantara [14]

Source: Author, 2024

From the above table, it is quite clear that machine learning (ML) is a popular AI technology.It is very popular because of its affirmed impact and multidimensional capacities in solving problems and optimizing a whole lot of things. This study argues here that given its commonly attested capacities, ML can be leveraged either independently or in combination with other AI technologies for the protection of CNI. Thapaliya and Bokani, [18] reveal that machine learning, deep learning, and natural language processing are AI techniques that can adequately tackle cyber security threats, empower security systems with massive data in real-time, identify the patterns of malicious activities, and automate incident response processes for proactive actions and efficient combat against threats.

Kalnawat's et al. [21] study shows that ML can safeguard CI against cyber threats, and calls for increased utilization of ML for such purposes. This means that the current extent of utilization is low. The need to increase the extent of utilization makes this study as well as the like others a dire necessity.Moreover, Ojo et al. [22] affirm the crucial role of AI technologies in addressing cyber security challenges, stressing their capacity to detect and predict cyber attacks and thereby prevent occurrences. They argue that blockchain, IoT, and autonomous technologies can be deployed to improve the resilience of critical systems [22] such as CNI.

Also, Volk [23] is of the view that since cyber security threats can be detected and prevented by AI technologies; there should be no hesitation to applying them wherever necessary for the attainment of safety.The National Strategy for Artificial Intelligence Bangladesh [NSAIB] (2020) indicates that AI technologies are capable of protecting critical infrastructure and improving the services of CI.In addition, the study by Yigit et al. (2018) observes that AI technologies have to be integrated into other measures or systems deployed for protecting CI in order to be able to quell cyber threats to CI. Obviously, AI technologies are known to perform various functions in different settings and endeavors. The Table 2 below contains a summary of the major functions of AI and ML in relation to the protection of CNI:

As evident in Table 2, AI plays diverse functions in various fields. The listed functions are the summation of the numerous functions played by AI as well as ML. For precision, the study sums up the many functions into the above, whereby some of the functions not mentioned fall under the above listed ones. Although the above listed functions are not considered exhaustive, they suffice for the many others. The base of the summation is the use of key conceptual representation for numerous concepts and thematic concerns.There are empirical studies lending credence to the foregoing. Accordingly, Adelani et al. [39] reveal that AI and ML can help mitigate cyber security threats to CI by virtue of their identification and prediction functions.

Binhammad et al. [1] demonstrate that AI based models are capable of organizing the networks for, and strengthening the functions of, infrastructure. The study calls on stakeholders to devise robust safety measures and constantly carry out audits to update CI. The present study makes the same call to that end.The study by Govea et al. [40] proves the ability of AI to proffer solutions through detection and prompt response

to cyber threats to energy infrastructure. It charges organizations and governments to leverage ML algorithms for prediction and detection of cyber security threats so as to proactively and significantly improve security management in energy infrastructure. The foregoing can obtain in other phases or sets of CI.

Adewusi et al. [41] demonstrate that human actions against cyber threats can be enhanced and optimized by AI. They call for more research and collaboration among professionals, institutions, enterprises and governments.They also call for vigorous frameworks that would foster and guide the deployment of AI for solutions in various endeavors.Similarly, Ojo and Aghaunor [12] show that cyber attacks on water and transport infrastructure can be foiled by AI technologies, if adopted and used appropriately. Their observation is factual and practically realizable. In another development, Peramo et al. [42] prove that ML can optimize workflows and resources like CI, and foster collaboration among professionals in finding solutions to issues, thereby enabling the realization of sustainable development goals. Clearly, the foregoing studies affirm the functional relevance of AI and ML in general and the protection of CNI in particular.

4. LEVERAGING AI AND ML FOR PROTECTION OF CNI

There is no doubt that AI and ML can be leveraged for the protection CNI across nations of the world. Since they are capable of improving security and optimizing performance in the maintenance of CNI, it is quite obvious that leveraging them for the protection of CNI can yield huge positive results. Sarker et al. [43] show that AI and ML optimize human interpretable decisions on security automation and intelligence for the protection of CI. This present study observes that their stated results apply to CNI, not CI alone. Kaur et al. [44] indicate that through critical and technical roles, such as threat detection and response, automation, accuracy of actions against cyber threats, and optimization, AI has been impacting positively on CI and offers better future opportunities for the development of CI in various regards.

Table 2. Summed up functions of AI and ML

Functions	Citations
Innovations	Akinola et al. [4]
Digitalization	Akinola [3]
Inventions and discoveries	Roshanaei et al. [24]
Optimization	Thuraka et al. [25]
Influencing effective planning	Singh [26]
Improving performance, services and operations	Obiuto et al. [5]
Enhancing teaching and learning	Kamble and Gaikwad [27]
Massive data creation, storage, dissemination and management	Regona et al. [8]
Data-driven decision-making	Juhrich [28]
Saving time and resources	Adefemi et al. [29]
Reducing costs	Mizrak [30]
Ensuring and increasing safety	Regona et al. [8]
Advancement	George et al. [31]
Accuracy and accountability	Bulama and Shirivastata [32]
Predictions and detections	Shaikh et al. [33]
Compliance management	Thakkar and Lohiya [34]
Incident reporting and response	Srivastava [35]
Mitigating challenges to environmental sustainability	Bidhendi and Azizi [36]
	Baker et al. [37]
	Vantara [14]
	Wang [38]
	Jarrahi [28]

Source: Author, 2024

Basically, AI and ML play essential role in optimizing operations, services, performance and results in all ramifications wherever they are integrated. Their roles in the protection of CNI include analyzing large amounts of data, identifying patterns, and making predictions that together enable organizations to respond effectively to threats. This study considers five major areas through AI and ML can help protect CNI. These are detection of and response to threats, facilitating efficient maintenance, assessing and managing risks, increased awareness, and simulation and training.

As these cutting edge technologies help protect the CNI of nations through optimization, detection, assessment and mitigation of risks, predictive maintenance of CNI, creation of awareness about situations and threats, and help in simulation and training of personnel, AI and ML ensure society's safety and wellbeing. This means that the protection of CNI correlates with the ensuring of society's safety and wellbeing. Doing so using AI and ML implies harnessing their huge prospects for maximal results in protecting CNI and ensuring safety, stability, growth, progress, and development of society. In what follows, each of them is given a brief on how AI and ML can be leveraged for the protection of CNI.

4.1 Detection of and Response to Threats

AI and ML algorithms can help to analyze system logs, detect anomalies, and network traffic. As they monitor these streams of data, they allow for identification of breaches in real-time and swift response to the mitigation of damages. ML models are capable of being trained to recognize normal patterns of behavior within a network. By so doing, the models would flag unusual activities that may pose cyber threats to CNI. Also, security systems driven by AI can automate the processes of incident response. The automation lessens the time spent on mitigating threats. Clearly, the impact of threats or attacks on CNI can be minimized by AI and ML. The foregoing points are captured in the following studies:Adelani et al. [39] Adewusi et al. [41] , Govea et al. [40] Kalnawat et al. [21] Ojo and Aghaunor [12] Ojo et al. [22] Okusi [16] Pasupuleti et al. [17] and Thapaliya and Bokani [18], among others.

4.2 Increased Awareness

With AI and ML, the level of awareness about real-time situations gets increased [15] Obinna et al., [45] NSAIB, 2020). Organizations are bound to understand their operational environment better, when they integrate AI, ML, social media and other cutting edge technologies into the creation of awareness about the situations at hand [15,45]. With high level of real-time situational awareness, decision-makers become capable of responding more effectively to incidents and coordinating resources in times of emergencies. For instance, in times of natural disasters, AI can help analyze weather forecast and sensor network data so as to predict the impact on CNI. This analysis by AI makes it possible for operators to take preventive measures for the protection of CNI and ensure the continuity of the services.

4.3 Simulation and Training

AI and ML can help in training personnel on how to handle and manage CNI efficiently [15,16,25] NSAIB, 2020). As they create simulations that are realistic in real-life situations of potential threats and incidents, AI and ML arm the organizations involved with skills and the capacity to effectively prepare their staff for facing highly demanding situations [14]. As such, employees of organizations in the CNI sector get trained and armed with technological literacy and technical skills for handling complex tasks with less stress and for solving difficult problems. Also, simulations make it possible for gaps in knowledge to be identified and bridged [42]. This point highlights the impact of AI and ML on knowledge, research and development, particularly as regards discourses on and matters concerning CNI. More so, by integrating AI and ML into training and simulation aimed at achieving the protection of CNI, optimized teaching and learning AI-driven programs help individuals to adapt to innovations.

4.4 Facilitating Efficient Maintenance

The efforts at maintaining the physical aspects of CNI can be facilitated by AI and ML. Predictions can be made about the maintenance of CNI by analyzing the data sensors implanted in equipment and infrastructure [46] Yigit et al., 2018). Since these predictions can reveal the possibility or impossibility of equipment breakdown, failure or success is determined. To that end, maintenance is made ahead to avert the occurrence of breakdown. For instance, in the power sector, AI can help in the analysis of data from power plants and transmission lines so as to predict equipment failures. The help makes

it possible for operators to tackle and avert potential disruptions. Of course, by so doing, the issues at stake are not left to escalate.

4.5 Assessing and Managing Risks

The extent to which risks are assessed and managed can be increased or made high(er) by AI and ML models [4,16,25] NSAIB, 2020). They analyze historical data and identify potential vulnerabilities in CNI. They also play a crucial role in the simulation of different threat scenarios, thereby helping organizations to better understand the level of their risk exposure. The exposure makes organizations to devise pragmatic strategies with which they can competently, promptly and adequately mitigate risks. The data-driven approach from AI and ML propels more effective decision-making on measures for the migration of risks obtains. In other words, the approach makes it possible for decision-makers to allocate resources more efficiently and give priority to investing in security measures. Also, organizations can become more adaptive to risk management and proactive or responsive to rising threats.

Practically, as Verma [47] notes, AI can be practically applied in the critical security of critical infrastructure, as in health facilities, financial institutions, transportation systems, and smart grid security operations that electrify utilities, and detect as well as respond to anomalies and potential threats to these utilities of national concern. Accordingly, AI and ML can be used in vehicles and for traffic purposes to monitor, detect and prevent anomalies. In the health sector, healthcare systems can be optimized with AI and ML algorithms. Patient data, services and satisfaction, and medical devices can be protected against cyber attacks, such as ransomware attacks that target hospital networks and IoT devices. Also, safeguarding finances and/or financial assets from cyber threats leads to the protection of CNI. The symbolic representation of the proposal of this study is typified in Fig. 2.

Studies express worries over the low extent of the utilization of AI and smart technologies in the industry [5] Alsakkaet al., 2023; Bidhendi & Azizi, [36] Oberer & Erkollar, [48,49] Given the expressed worries, this study argues that AI and ML are yet to be leveraged adequately for the protection of CNI. The need to do so is what informed this study. Regardless of the inherent challenges, the utilization of AI adoption in various spheres can still be increased once stakeholders duly rise to the challenges and combat them head-on.

Although there is no doubt that AI and ML can optimally address the challenges of CNI and solve a range of problems in different spheres of life, there are attendant issues [23,50]. These include emerging and growing cyber security threats or attacks, data privacy intrusion and hijack, identity theft, and abusive use of AI. As these threats become increasingly alarming, governments, organizations and individuals have to consistently rise to the challenges by being sensitive to cyber security threats, and devising technology-based measures for mitigating them. These include working out stringent modalities

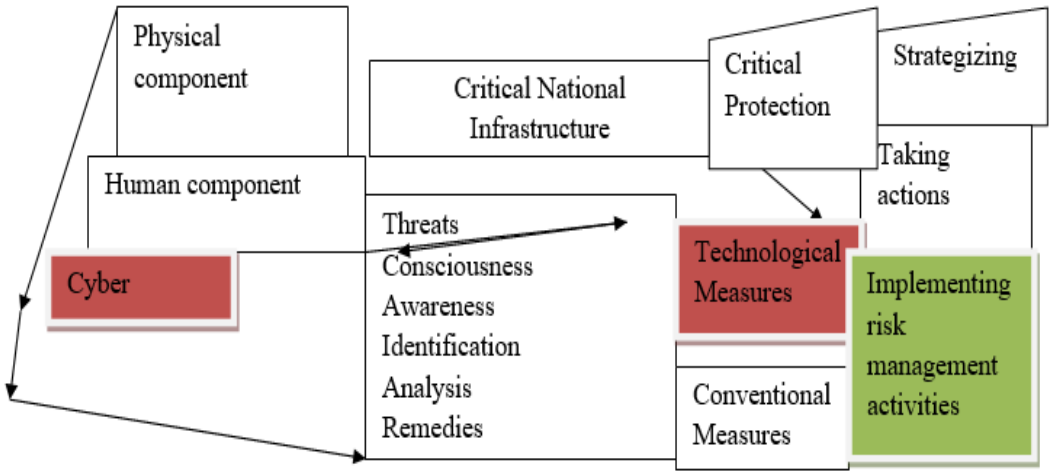

Fig. 2. Surmounting challenges to AI adoption to increase utilization
Source: Author, 2024

and operational legations for lasting solutions and prevention. There are also issues of transparency and accountability in decision-making involving the use of AI and ML for the protection of CNI. Volk [23,51] observes that interconnectedness of AI technologies, their complexities, and the trend of digitalization makeAI and ML vulnerable to cybercriminals.

Besides, huge finance, skilled personnel, and expensive logistics are needed for significant and functional integration of AI and ML into endeavors like the protection of CNI. This study argues that regardless of these challenges to the adoption of AI and ML, their integration is overwhelmingly imperative and wholesomely beneficial. Given this reality, failing to adopt these cutting edge technologies for purposes such as the protection of CNI means not taking advantage of their huge prospects and failing to harness them for solutions to problems that they can help address more effectively than the conventional mechanisms could do. It is ideal for organizations to adopt them and consistently find ways of mitigating the challenges so as to tap from the huge prospects of these cutting edge technologies, as in leveraging AI and ML for optimal protection of CNI in all nations of the globe. It is important to note that just as Verma [47,52,53] emphasizes, the adoption of AI technologies for critical security should be combined with other strategic measures, technology-based and non-technology alike. These include rethinking policies on establishment, operations and protection of CNI, and repositioning, redesigning and re-strategizing security measures on regular basis.

5. CONCLUSION

The significance of critical national infrastructure (CNI) across the globe cannot be overemphasized. Being of global significance, issues concerning or affecting them are of great national concern. Therefore, to proffer tangible solutions to the challenges of CNI in both developed and developing nations, this study proposes the significant leveraging of artificial intelligence (AI) and machine learning (ML) for the protection of CNI. It posits that although other conventional measures for protecting CNI abound, leveraging AI and ML for the protection of CNI would yield more results, address the inherent challenges more significantly, and optimize the conventional measures for maximal results.

The novelty of the study rests on its projection of AI and ML for the protection of CNI, showing scholarly evidence to that end. The paper demonstrates that as AI and ML algorithms automate repetitive and time-consuming tasks, the allocation of resources becomes more efficient, businesses get streamlined, and cost-savings, productivity and improved standard of living obtain increasingly. Drawing evidence from extant studies, the present study shows that when leveraged judiciously, AI and ML can play a critical role in the protection of CNI.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Option 1: Author hereby declares that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

COMPETING INTERESTS

Author has declared that they have no known competing financial interests or non-financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

1. Binhammad M, Alqaydi S, Othman A, Abuljadayel LH. The role of AI in cyber security: Safeguarding digital identity. Journal of Information Security. 2024;15:245-278. Available:https://doi.org/10.4236/jis.2024.152015
2. Yu C. AI as critical infrastructure: Safeguarding national security in the age of artificial intelligence. Preprint. 2024;1-16. Available:http://doi:org/10.31219/osf.io/u4kdg
3. Akinola AP. Leveraging cost-effective AI and smart technologies for rapid infrastructural development in USA. African Journal of Advances in Science and Technology Research. 2024;15(1):59-71. Available:https://doi.org/10.62154/rktd4f30
4. Akinola AP, Thuraka B, Okpeseyi SBA. Achieving housing affordability in the U.S. through sustained use of AI and robotic process automation for prefabricated modular construction. African Journal of Advances in Science and Technology Research. 2024;15(1):122-134.

Available:https://doi.org/10.62154/53t99n63

5. Obiuto NC, Adebayo RA, Olajiga OK, Festus-Ikhuoria IC. Integrating artificial intelligence in construction management: Improving project efficiency and cost effectiveness. Int. J. Adv. Multidisc. Res. Stud. 2024;4(2):639-647.
6. Juhrich SS. Real-time safety technologies in the construction industry: A study of current state and challenges. Industrial design engineering, Master's Level 2023, Department of Business Administration, Technology and Social Sciences, Luleå University of Technology; 2023.
7. Ivanova S, Kuznetsov A, Zverev R, Rada A. Artificial intelligence methods for the construction and management of buildings. Sensors. 2023;23(21):8740.
8. Regona M, Yigitcanlar T, Xia B, Li RYM. Opportunities and adoption challenges of AI in the construction industry: A PRISMA review. Journal of Open Innovation: Technology, Market, and Complexity, 8(1), Article number 45; 2022.
9. Kochovski P, Stankovski V. Building applications for smart and safe construction with the DECENTER fog computing and brokerage platform. Automation in Construction. 2021;1;124:103562.
10. Yigitcanlar T, Desouza KC, Butler L, Roozkhosh F. Contributions and risks of artificial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature. Energies. 2020;13(6).
DOI: 10.3390/en13061473
11. Mustyala A. Artificial intelligence and machine learning in infrastructure security whitepaper. International Journal of Science and Research (IJSR). 2023;12(10):868-870.
DOI: 10.21275/SR231005100307
12. Ojo B, Aghaunor CT. AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. International Journal of Science and Research Archive. 2024;12(02):1716–1726.
Available:https://doi.org/10.30574/ijsra.2024.12.2.1401
13. Mittelsteadt M. Critical risks: Rethinking critical infrastructure policy for targeted AI regulation. Policy Brief, Mercatus Center, George Mason University; 2024.
14. Vantara H. AI and machine learning initiatives for data center modernization. White Paper, WP-575-C BTD; 2020.
15. Kodete CS, Thuraka B, Pasupuleti V, Malisetty S. Determining the efficacy of machine learning strategies in quelling cyber security threats: Evidence from selected literatures. Asian Journal of Research in Computer Science. 2024;17(7):168-77.
Available:https://doi.org/10.9734/ajrcos/2024/v17i7487
16. Okusi O. Cyber security techniques for detecting and preventing cross-site scripting attacks. World Journal of Innovation and Modern Technology. 2024;8(2):71-89.
DOI: 10.56201/wjimt.v8.no2.2024.pg71.89
17. Pasupuleti V, Thuraka B, Kodete CS, Malisetty S. Enhancing supply chain agility and sustainability through machine learning: Optimization techniques for logistics and inventory management. Logistics. 2024;8(73).
Available:https://doi.org/10.3390/logistics8030073
18. Thapaliya S, Bokani A. Leveraging artificial intelligence for enhanced cybersecurity: Insights and innovations. Sadgamaya. 2024;1(1):46-53.
19. Alsakka F, Assaf S, El-Chami I, Al-Hussein M. Computer vision applications in offsite construction. Automation in Construction. 2023;154:104980.
20. Wusu GE, Alaka H, Yusuf W, Mporas I, Toriola-Coker L, Oseghale R. A machine learning approach for predicting critical factors determining adoption of offsite construction in Nigeria. Smart and Sustainable Built Environment (ahead-of-print); 2022.
21. Kalnawat A, Dhabliya D, Vydehi K, Dhablia A, Kumar SD. Safeguarding critical infrastructures: Machine learning in cybersecurity. (ICECS'24) E3S Web of Conferences. 2024;491:02025.
Available:https://doi.org/10.1051/e3sconf/202449102025
22. Ojo B, Ogborigbo JC, Okafor MO. Innovative solutions for critical infrastructure resilience against cyber-physical attacks. World Journal of Advanced Research and Reviews. 2024;22(03):1651–1674.
Available:https://doi.org/10.30574/wjarr.2024.22.3.1921

23. Volk M. A safer future: Leveraging the AI power to improve the cybersecurity in critical infrastructures. Elektrotehniški Vestnik. 2024;91(3):73-94.
24. Roshanaei M, Khan MR, Sylvester NN. Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions. Journal of Information Security. 2024;15:320-339. Available:https://doi.org/10.4236/jis.2024.153019
25. Thuraka B, Pasupuleti V, Malisetty S, Ogirri KO. Leveraging artificial intelligence and strategic management for success in inter/national projects in US and beyond. Journal of Engineering Research and Reports. 2024;26(8):49-59. Available:https://doi.org/10.9734/jerr/2024/v26i81228
26. Singh S. Benefits of an AI enabled safety management system in construction. Upload on Research Gate; 2024.
27. Kamble K, Gaikwad M. Detection of construction safety and accident management using AI. International Research Journal of Modernization in Engineering Technology and Science. 2024;06(01).
28. Jarrahi MH. Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. Business Horizons. 2018;61(4):577-586.
29. Adefemi A, Ukpoju EA, Adekoya O, Abatan A, Adegbite AO. Artificial intelligence in environmental health and public safety: A comprehensive review of USA strategies. World Journal of Advanced Research and Reviews; 2023.
30. Mizrak F. Integrating cybersecurity risk management into strategic management: A comprehensive literature review. Research Journal of Business and Management (RJBM). 2023;10(3):98-108. Available:http://doi.org/10.17261/Pressacademia.2023.1807
31. George RM, Nalluri MR, Anand KB. Application of ensemble machine learning for construction safety risk assessment. J. Inst. Eng. India, Ser. A. 2022;103:989-1003. Available:https://doi.org/10.1007/s40030-022-00690-w
32. Bulama L, Shirivastata M. The role of information and communication technology towards protection of lives and property in northern Nigeria: A focus on Maiduguri Borno State in vidyabharti. International Interdisciplinary Research Journal. 2022;14(1):1–9.
33. Shaikh AA, Kumar A, Jani K, Mitra S, García-Tadeo DA, Devarajan A. The role of machine learning and artificial intelligence for making a digital classroom and its sustainable impact on education during covid-19. Materials Today: Proceedings. 2022;56:3211–3215. Available:https://doi.org/10.1016/j.matpr.2021.09.368
34. Thakkar A, Lohiya R. A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions. Artificial Intell Rev. 2021;55(1):453–563. Available:https://doi.org/10.1007/S10462-021-10037-9
35. Srivastava A. The application and impact of artificial intelligence (AI) on E-commerce. Contemporary Issues in Commerce and Management. 2021;1(1): 165-75.
36. Bidhendi A, Azizi M. Application of machine learning in project management. 12th International Congress on Civil Engineering, Ferdowsi University of Mashhad, Mashhad, Iran; 2021.
37. Baker SR, Bloom N, Davis SJ, Terry SJ. Covid-induced economic uncertainty. National Bureau of Economic Research, no. 26983, 1-16. JEL No. D80,E17,E32,E66,L50; 2020.
38. Wang P. On defining artificial intelligence. Journal of Artificial General Intelligence. 2019;10(2):1-37.
39. Adelani FA,Okafor ES, Jacks BS, Ajala OA. Theoretical frameworks for the role of AI and machine learning in water cybersecurity: Insights from African and U.S. applications. Computer Science and IT Research Journal. 2024;5(3):681-692. DOI: 10.51594/csitrj.v5i3.928
40. Govea J, Gaibor-Naranjo W, Villegas-Ch W. Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. Systems. 2024;12:165. Available:https://doi.org/10.3390/systems12050165
41. Adewusi AO, Okoli UI, Olorunsogo T, Adaga E, Daraojimba DO, Obi OC. Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA

review. World Journal of Advanced Research and Reviews. 2024;21(01): 2263–2275.
Available:https://doi.org/10.30574/wjarr.2024.21.1.0313

42. Peramo EC, Jr Piedad E, De Leon FA. Advancing national development through AI: Policy recommendations for enhancing AI research and applications in the Philippines. Case Study for the Multistakeholder Forum on Science, Technology and Innovation for the SDGs. 2024;1-5.
43. Sarker IH, Janicke H, Ferrag MA, Abuadbba A. Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures. Internet of Things. 2024;25:101110.
Available:https://doi.org/10.1016/j.iot.2024.101110
44. Kaur, Gabrijelˇciˇc R, Klobuˇcar T. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion. 2023;97:101804.
Available:https://doi.org/10.1016/j.inffus.2023.101804
45. Obinna NN, Thuraka B, Okusi O. Impact of information technology on teaching and learning: A focus on hybrid teaching mode. African Journal of Humanities and Contemporary EducatioN Research. 2024;15(1):119-130.
Available:https://doi.org/10.62154/689nh583
46. Mungoli N. Leveraging AI and technology to address the challenges of underdeveloped countries. J Electrical Electron Eng. 2023;2(3):211-216.
47. Verma D. Enhancing critical infrastructure security through artificial intelligence. LinkedIn Post; 2024.
Available:https://www.linkedin.com/pulse/title-enhancing-critical- infrastructure-security-through-verma-dp2zc
48. Oberer B, Erkollar A. Leadership 4.0: Digital leaders in the age of industry 4.0. International Journal of Organizational Leadership. 2018;7(4):404-412.
DOI: 10.33844/ijol.2018.60332
49. Zhang D. Challenges of formation damage control technology for ultra-deep tight gas reservoirs: A case study from Tarim Basin. Next Sustainability. 2024;4:100046.
Available:https://doi.org/10.1016/j.nxsust.2024.100046
50. Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. Energy Reports. 2021;7:8176–8186.
Available:https://doi.org/10.1016/j.egyr.2021.08.126
51. National Strategy for Artificial Intelligence Bangladesh. Information and communication technology division government of the people's republic of Bangladesh; 2020.
52. Regona M, Yigitcanlar T, Hon CKH, Teo M. Mapping two decades of AI in construction research: A scientometric analysis from the sustainability and construction phases lenses. Buildings. 2023;13:2346.
Available:https://doi.org/10.3390/buildings13092346
53. Yigit Y, Ferrag MA, Sarker IH, Maglaras LA, Chrysoulas C, Moradpoor N, Janicke H. Critical infrastructure protection: Generative AI, challenges, and opportunities. IEEE Journal. 2016;4:1-14.
DOI: 10.1109/ACCESS.2017

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/124252