Journal of Mathematics and Statistics Studies
ISSN: 2709-4200
DOI: 10.32996/jmss
Journal Homepage: www.al-kindipublisher.com/index.php/jmss

JMSS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Mathematical and AI-Blockchain Integrated Framework for Strengthening Cybersecurity in National Critical Infrastructure

Md Mahababul Alam Rony[1] ✉ Md Shadman Soumik[2] and MAHINUR SAZIB SRISTY[3]
[1]Master of Science in Computer Science, Washington University of Virginia
[2]Master of Science in Information Technology, Washington University of Science & Technology
[3]Bachelor of Science in Computer Science and Engineering, North South University
Corresponding Author: Md Mahababul Alam Rony, **E-mail**: mr23437@wuv.edu

| ABSTRACT
This article examines the intersection between mathematical modeling, artificial intelligence (AI), and blockchain technology as a way of strengthening cybersecurity in national critical infrastructures (NCI). The increasing frequency and sophistication of cyber threats against vital infrastructures, such as electrical grids, healthcare information networks, and transportation infrastructures, creates the need to develop some innovative protective mechanisms. To solve these concerns, in the article the authors propose a hybrid framework that combines the AI-driven predictive analysis and the decentralized ledger capabilities of blockchain technology. Decentralized ledger technology (DLT) forms the backbone of secure and tamper-proof data management and machine learning algorithms are used to identify and predict emerging threats in real-time. By combining the immutability of the blockchain technology and the adaptive analytical capabilities of AI, this framework aims to improve the integrity of the data, maintain the privacy of it, and provide a fast-responding mechanism in the NCI environments. The paper outlines possible applications, lists the benefits that come with such applications, and addresses challenges inherent in the implementation of such an integrated system in order to provide a blueprint for future scholarly investigation and practical implementation.

| KEYWORDS

AI, Blockchain, Cybersecurity, Critical Infrastructure, Mathematical Framework, Decentralized Ledger Technology, Machine Learning.

| ARTICLE INFORMATION

ACCEPTED: 01 May 2023 **PUBLISHED:** 20 May 2023 **DOI:** 10.32996/jmss.2023.4.2.10

1. Introduction

The growing dependence on digital systems used in national critical infrastructures (NCIs) has increased the vulnerability of critical societal functions to cyber threats. These infrastructures, which include energy grids, healthcare systems, transportation networks, water supply systems, financial networks, are necessary to support the maintenance of civilian welfare and security. As their interconnectivity and their technological dependency grow stronger, they simultaneously become tempting targets for cyber-attacks, thus placing cybersecurity at the top of governmental and organizational priorities worldwide.

National critical infrastructures face a range of cyber threats from data breaches and ransomware to sophisticated advanced persistent threats (APTs) meant to disrupt operations and cause significant economic and social damage. Conventional methods of cybersecurity, however, are often reactive and fragmented and are insufficient to meet the growing complexity and scale of these threats. Consequently, the development of cyber-attacks has led to the exploration of new, innovative, and integrated solutions that could proactively defend against the attack of NCIs.

Artificial Intelligence (AI) and Blockchain technologies are among the promising candidates capable of mitigating cybersecurity challenges in NCIs. Their integration promises to transform the cybersecurity landscape with its capability for intelligent decision making coupled with the security, transparency and immutability of data handling. Nonetheless, the incorporation of these technologies into the existing NCI infrastructures, as well as the use of mathematical frameworks to model and optimize performance of these systems, is an evolving research frontier.

1.1 Role of AI in Cybersecurity in NCIs

AI plays an ever-increasing role in cybersecurity because the amount of data has grown and so has the complexity of threats. Traditional methods of defense usually rely on predetermined rules and signature patterns to detect known threats and, again, such methods fail when faced with novel, undocumented or changing adversaries that require a dynamic, evolving defense. A subset of AI, machine learning (ML) algorithms can analyze a large amount of data in real time, detecting patterns and anomalies that indicate a possible security breach. By taking advantage of the information related to historical attacks, ML models become very good at identifying emerging attack vectors, which in turn helps to mitigate attacks in a proactive manner.

Additionally, AI enables automated cybersecurity processes which can lower the response latencies and increase the efficiency of the operations. For example, systems powered by artificial intelligence (AI) can autonomously detect intrusions and identify vulnerabilities and appropriate remediation strategies, and an AI-powered system can take action even without human intervention, which can be especially important for maintaining NCI continuity in the wake of timely threats.

$$P(\text{Attack}) = \sum_{i=1}^{n} \alpha_i \cdot P(\text{Threat}_i)$$

This formula calculates the overall probability of a cyber-attack occurring by aggregating the individual threat probabilities. Each threat is weighted by its significance (denoted as a_1) providing a comprehensive prediction of potential attacks based on multiple data points and threat vectors.

Deep learning (DL) architectures (more specifically, neural networks) are known to be excellent at detecting sophisticated cyber-attacks (such as zero day exploits and APTs) that attempt to circumvent conventional defence mechanisms. Continuous learning from small data helps the predictive power of DL systems to become more accurate, which means that threat detection becomes more powerful over time.

1.2 Blockchain Technology vs Cybersecurity

Blockchain technology, originally invented to be used as the foundation for cryptocurrencies like Bitcoin, has garnered interest for its potential to revolutionize a number of different industries, cybersecurity included. At a very basic level, Blockchain forms a decentralized ledger that is distributed among a network and stores data in an immutability and transparency approach. Each block contains a cryptographically secured transaction history which is associated with the previous block and creates an unchangeable chain. This architecture makes tampering data virtually impossible without network consensus.

Within the field of cybersecurity, the Blockchain offers several benefits that help build NCI resilience. First, its decentralization, which eliminates single points of failure, promoting greater resistance to distributed denial-of-service (DDoS) attacks and data breaches, supporting this need for continuous availability required by critical infrastructure. Second, Blockchain ensures data integrity via the cryptographic proof, i.e., once the data is recorded the information cannot be changed or deleted, making auditability, traceability, and accountability of unauthorized actions possible. Third, blockchain-based identity management systems can be used to authenticate and authorize users and devices to ensure that access to sensitive NCI assets is limited to legitimate actors.

1.3 Blockchain and AI: How Can They Enhance Cybersecurity?

While AI and Blockchain separately tackle different cybersecurity issues, the convergence of the two provides a more powerful, adaptive approach to security for NCIs. The dynamic decision-making capability of AI merged with the secure data provenance of Blockchain will be able to build a synergistic solution to complex threat environments. AI can use Blockchain to record its decisions and thus create immutability audit trails to increase accountability, a key imperative when AI-controlled controls affect critical infrastructure operations.

On the contrary, AI can help in enhancing the functionality of Blockchain as it can be used to optimize computational resources, predict the outcomes of transactions, identify anomalies in real-time, and suggest optimal consensus strategies, thereby reducing the computational overhead that is inherent in Blockchain operations.

Furthermore, AI can anticipate possible vulnerabilities existing in Blockchain systems by analyzing historical data sets of cyber attacks and using pattern recognition to foster proactive defense measures and reduce the likelihood of breaches.

1.4 Mathematical Framework of the Optimization of AI-Blockchain Integration

The amalgamation of AI and Blockchain into an integrated cybersecurity architecture is successful only if it has a strong mathematical foundation. Optimization algorithms can be used to find an efficient allocation of computing resources between AI and Blockchain components. Game theoretical and decision theoretical models offer insights into stakeholder cooperation for cost effective cyber security enhancement. Additionally, performance characteristics, such as detection efficacy, response latency, system availability, and data privacy, can be tested by mechanistic modelling of AI algorithms and Blockchain protocols, which can be used to simulate attack scenarios and test defence efficacy.

$$\text{Maximize:} \quad \sum_{i=1}^{m} \text{Accuracy}_i - \lambda \cdot \sum_{j=1}^{n} \text{Latency}_j$$

This formula represents the optimization process of balancing the detection accuracy and response latency in the integrated AI-Blockchain framework. The goal is to maximize accuracy in threat detection while minimizing the latency of responses, ensuring a fast and effective cybersecurity system.

1.5 Challenges in the Way Forward

Despite the great potential of AI - Blockchain integration to NCI cybersecurity, there are several challenges that remain. Scalability comes first of all; both the AI and Blockchain require extensive computational resources, and this raises the concern about efficient operation at the national infrastructure scale. As the volumes, rates, and temporalities of the data generated by NCIs are vast, optimising the technologies used to manage them is imperative.

Integration of Artificial Intelligence and Blockchain in legacy NCI systems is another obstacle. Existing infrastructures were built before these paradigms came into existence so retrofitting is technically complex and financially onerous. Adoption also requires wide-ranging changes to governance, policy, and regulatory frameworks and could hamper the widespread deployment.

Finally, trust and accountability issues arise due to the convergence of AI and Blockchain. While Blockchain provides strong data integrity, many Artificial Intelligence algorithms are kept in black boxes making it difficult to understand the entire decision-making process. Establishing transparent and accountable systems of AI-based cybersecurity is a must, especially in high-stakes NCI situations.

2. Literature Review

The integration of Artificial Intelligence (AI) and Blockchain technologies to improve cybersecurity for the national critical infrastructures (NCIs) is a nascent yet promising field of concern in academia. The combination of these technologies helps to address salient vulnerabilities inherent in the conventional cybersecurity frameworks, thereby providing a more secure, transparent and intelligent paradigm to the protection of critical systems. This literature review systematically analyzes recent research on AI and Blockchain in the cybersecurity context, outlines their respective contributions, highlights challenges in integrating the two and describes potential applications in NCIs.

2.1 The Importance of Artificial Intelligence in Cybersecurity.

Artificial Intelligence, especially Machine Learning (ML) and Deep Learning (DL), has become an indispensable tool to enhance the cybersecurity capabilities. Traditional cybersecurity systems, which depend on rule-based systems and predefined signatures, are not well prepared to counter novel or sophisticated cyber-attacks. On the contrary, AI provides the ability to learn from past data, adapt to emerging threats and identify anomalies in real time.

AI-powered systems are able to analyze large amounts of data produced by NCIs, thus detecting potential threats - such as malware, phishing attacks and Distributed Denial of Service (DDoS) attempts. Supervised learning algorithms, which are used for ML models, are especially useful in the detection of known threats by classifying them on the basis of historical data. Nonetheless, the power of AI comes in the fact that it can detect zero day exploits and advanced persistent threats (APTs) that bypass traditional signature-based systems. For example, deep learning methods, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), have been employed to identify more complex patterns and behaviors in network traffic, which can help improve security capabilities (Buczak & Guven, 2016).

An increasing body of research makes it clear why predictive analytics is needed, in which AI can anticipate possible attacks based on network behaviours and vulnerabilities. Empirical studies by O'Neill et al. (2018) and Wang et al. (2020) provide examples of training AI models to predict vulnerabilities and security breaches before they happen, in order to provide proactive as opposed to reactive defence mechanisms.

2.2 Blockchain and Its Role in Cyber security

Blockchain was initially developed for cryptocurrency based transactions, but has now made a significant leap in securing data in a decentralized and unchangeable way. Its application to cybersecurity is based on its ability to provide data integrity, transparency, and trust. By ensuring that the data of a recorded datum cannot be changed or removed without consensus from the network, Blockchain offers a mechanism for preventing unauthorized changes - an essential feature for protecting NCIs.

The transparency and auditability that comes with Blockchain makes it especially ideal for securing communication and transactions in important infrastructure systems. The development of a decentralized ledger that logs all transactions, communications, or events that occur makes sure that the data access and alterations to the system remain both auditable and tamper-proof. This attribute is particularly important for infrastructures that demand constant availability such as power grids or transportation networks where unauthorised changes can lead to catastrophic results.

Moreover, the distributed nature of Blockchain reduces the risk that a single point of failure will occur. In centralized systems, compromise of the central server or database grants unfettered access to the entire system to the adversaries. With Blockchain, data spreads across several nodes providing more resilience against DDoS and ransomware attacks. Blockchain also allows for safe identity management and access control to ensure that only the authorised users and devices are able to access sensitive infrastructure systems (Zohar & Weitzner, 2018).

Research by Zhang et al. (2020) emphasizes on Blockchain's potential for providing security in communication between devices in Internet of Things (IoT) based critical infrastructure systems, where traditional security can be insufficient.

2.3 Integration of AI and Block Chain for Cybersecurity

The combination of AI and Blockchain is a new paradigm for cybersecurity in NCIs. By combining the prediction power of AI with the unmanipulable data storage of Blockchain, the amalgamation product provides greater resilience against cyber threats.

One of the major problems in cybersecurity is the ability to respond to threats in real-time while maintaining data integrity. AI in isolation can support real time threat detection and response, but can still be tampered with or data can be manipulated, especially if the data used to train the AI are corrupted. Blockchain can improve this weakness by ensuring that the data used for decision-making is secure and unaltered. Consequently, the immutability nature of Blockchain ensures that AI models are working with legitimate information which provides an extra layer of safety.

A study conducted by Zhang et al. (2021) suggests that AI can predict the probability of an attack, whereas Blockchain is used to record and audit all actions performed by the AI system. This combination of predictive capability and transparency can help to increase confidence in AI-driven cybersecurity systems, especially in industries such as finance, healthcare and energy, where the consequences of data breaches are serious.

In their study of federated learning, Rausch et al. (2020) showed that it is possible to train AI models with data distributed across different datasets without exposing data to external repositories. This principle is particularly relevant for BlockChain-based systems, where privacy and security of data are of prime importance. Federated learning when amalgamated with Blockchain allows for the secure and privacy preserving training of AI, making it an ideal candidate for critical infrastructure.

2.4 Applications In Critical Infrastructures

The combination of AI and Blockchain is especially effective in strengthening NCIs because they often face specific security challenges that can be attributed to their size, complexity, and importance. In the energy sector, AI will be able to predict faults and failures among smart grids, whereas Blockchain will record and audit all the mitigation actions being taken, which will increase the security and efficiency of energy distribution as well as provide a transparent audit trail for regulatory compliance.
Within the healthcare domain, AI can be used to identify abnormal patterns in patient data or medical records that may indicate security breaches or fraudulent activity. Blockchain protects patient information by ensuring it is confidential and uneditable and in line with privacy laws such as GDPR and HIPAA. In transportation, AI can help predict and prevent cyber-attacks on autonomous vehicles and smart transportation networks, while Blockchain is used to track the history of vehicles and their sensor data to ensure that they are tamper-proof.

2.5 Challenges and Limitations

Despite the promise embodied in the AI Blockchain hybrid, there are a number of challenges that need to be overcome to make this approach pragmatic for widespread implementation. Chief among the latter is scalability. Blockchain networks using consensus mechanisms like Proof of Work (PoW) can be slow and have high computational requirements. Scaling Blockchain systems to handle the large data volumes produced by NCIs, e.g. real time sensor data or network traffic, requires a great deal of optimisation and innovation.

Another challenge is concerned with the complexity of integrating AI and Blockchain in preexisting NCI infrastructure. Many critical infrastructures use legacy systems that have not been designed to integrate with modern technologies such as AI and Blockchain. Retrofitting these systems to work with AI and Blockchain can be expensive and time consuming as well as potentially introducing new vulnerabilities if not performed correctly.

Finally, there is the issue of trust in AI models. While Blockchain can serve as a way to have an unalterable audit trail, because of the "black-black" character of many AI algorithms, it is difficult to understand decision-making processes. This opacity represents a barrier to its widespread use, especially in sectors where accountability and explainability are paramount, such as healthcare and finance.

Table 1: Comparison of AI and Blockchain in Cybersecurity

Feature	**AI**	**Blockchain**
Main Strength	Predictive threat detection and response	Data integrity, transparency, and decentralization
Data Handling	Processes and analyzes data to identify anomalies	Stores data securely in an immutable ledger
Scalability	Can handle large datasets but computationally expensive	Can be slow and resource-intensive, especially with PoW
Real-time Response	Can provide real-time decision-making and automation	Offers transparency but cannot respond in real-time
Data Privacy	Can be vulnerable to manipulation if data is compromised	Ensures data privacy through decentralization and cryptographic methods
Key Application	Threat detection, predictive analytics, anomaly detection	Secure data storage, identity management, auditability
Limitations	Vulnerable to adversarial attacks and data manipulation	Slower transaction speeds, scalability issues

The table summarizes the main strengths, data handling capabilities, scalability, real-time response, data privacy, and key applications of AI and Blockchain in cybersecurity. It highlights the complementary nature of both technologies, where AI excels in dynamic decision-making and Blockchain offers strong data integrity and transparency.

3. Methodology

The methodology of Artificial Intelligence (AI) and Blockchain integration for strengthening cybersecurity in National Critical Infrastructures (NCIs) uses the systematic and multi-phased approach that combines theoretical constructs, empirical data analysis, and case study methodology. The goal is to show how the hybrid architecture AI - Blockchain can be operationalised to protect critical infrastructure in order to deliver a more efficient and transparent cybersecurity solution.

3.1 Framework Development

The first step in this methodology is designing a hybrid framework of AI & Blockchain sensitive to the special needs of NCIs. This involves the choice of the most appropriate AI techniques and Blockchain protocols to manage the unique security challenges of critical infrastructures.

3.1.1 AI Techniques Selection

For the AI part, different machine learning and deep learning algorithms are tested based on their ability to deal with different types of cyber threats, such as malware detection, intrusion detection, anomaly detection and attack prediction. The selected methods of Artificial intelligence are:

Supervised Learning Algorithms: Algorithms that are used for classification problems, such as known threats, from labelled data. Decision trees, support vector machines (SVM) and random forest are analyzed in terms of anomaly detection in network traffic.

Unsupervised Learning Algorithms In order to detect unknown threats or unusual patterns that were not labelled before, unsupervised learning techniques such as clustering (e.g. K- means) and autoencoders are used.

Deep Learning (DL): Convolutional Neural Networks (CNNs) and Long Short -Term Memory networks (LSTMs) are chosen to identify more sophisticated cyber threats such as advanced persistent threats (APTs) and zero -day exploits by analysing sequential data from NCIs.

3.1.2 Protocols Selection of Blockchain

The BlockChain component is aimed at ensuring data integrity, transparency and security. Appropriate Blockchain protocols are selected according to how it can deliver immutability, decentralisation and security for critical infrastructure systems. For the proposed solution, the Blockchain categories are considered as follows:

Private Blockchain: A permissioned Blockchain controls the network participation & transaction validation and thus protects sensitive infrastructure data. Hyperledger Fabric is often used in private Blockchains in industrial applications because of the modular architecture.

Smart Contracts: Smart contracts are embedded to automate security protocols and ensure that actions performed by AI systems (e.g. mitigation of detected threats) are in accordance with predefined rules without the need for intermediary involvement.

Blockchain Consensus Mechanisms: Proof of Authority (PoA) is used in preference to Proof of Work (PoW) because of its lower computational overhead and suitability for Blockchain applications where enterprise-level features are needed.

3.2 System Architecture Design

A key feature of the methodology is the creation of a system architecture that combines both AI and Blockchain technologies. This step involves developing a secure and scalable platform that can handle the computational demands of these technologies.

3.2.1 System Components

The architecture is conceived as a hybrid platform that contains the following elements:

Data Sources: Sensors, devices, and existing infrastructure monitoring systems within NCIs are the raw data which is collected and stored for later analysis.

AI Module: This module processes the collected data by using machine - learning and deep learning models in order to detect anomalies, predict potential attacks, and generate alerts for human analysts.

Blockchain Ledger: The Blockchain acts as a secure and unchangeable record keeping system, where AI generated actions (e.g. detection alerts and mitigation steps) and the results of such action can be stored, providing auditability and transparency.

User Interface (UI): Dashboard or control panel that is designed for the use of cybersecurity personnel designed to visualise the insights from the AI, threats alerts and Blockchain records, allowing real time monitoring of the security of the infrastructure and the activities of the system in a real time manner.

3.2.2 Data Flow and Interaction

The flow of data in the system is defined as follows:
Data Collection: Real time data is obtained from different NCI sources including sensor outputs, traffic logs and operational status reports.

Data Preprocessing: The gathered data is then subject to a preprocessing, such as normalisation, feature extraction and reduction of noise, to make it ready for AI analysis.

AI Analysis: AI algorithms are applied to the pre-processed data to identify the possible security threats, anomalies and vulnerabilities. Both the supervised and unsupervised learning techniques are used to classify data and find patterns that indicate attacks.

Blockchain Recording: After an anomaly or possible attack is detected, the involved data (including the AI's decision) is logged to the Blockchain to ensure transparency and immutability.

Action and Feedback: Once Blockchain recordation has taken place, automated mitigation action, as dictated by smart contracts, is taken. Feed back from these actions is sent back to the AI system which helps it fine-tune its predictive capabilities.

3.3 Experimental Setup

3.3.1 Data Set Collection

To test the AI-"Blockchain" framework, a dataset of real-world environments in the form of NCIs or simulated environments is needed. Data can be taken from publicly available cybersecurity datasets (e.g. the KDD Cup 1999 dataset, UNSW-NB15), as well as gaining access to real time data from smart grid simulation or IoT based security systems.

Attack Types: The dataset should include both benign traffic and attack examples, such as network intrusions, DDoS attacks, malware propagation, and unauthorised access attempts.

Data Segmentation: The information is divided into training and testing to measure model performance with the testing data simulating real-time cyber-attacks on NCI.

3.3.2 Evaluation Metrics

To measure the performance of the AI - Blockchain framework, the following metrics are used:

Accuracy: The percentage of accurate predictions that are made by the AI system.

Precision and Recall: Measures of the AI's ability to recognise true positives and false positives as little as possible.

F1 Score: F1 Score is the harmonic mean of precision and recall in a way that it balances the false positives and false negatives.

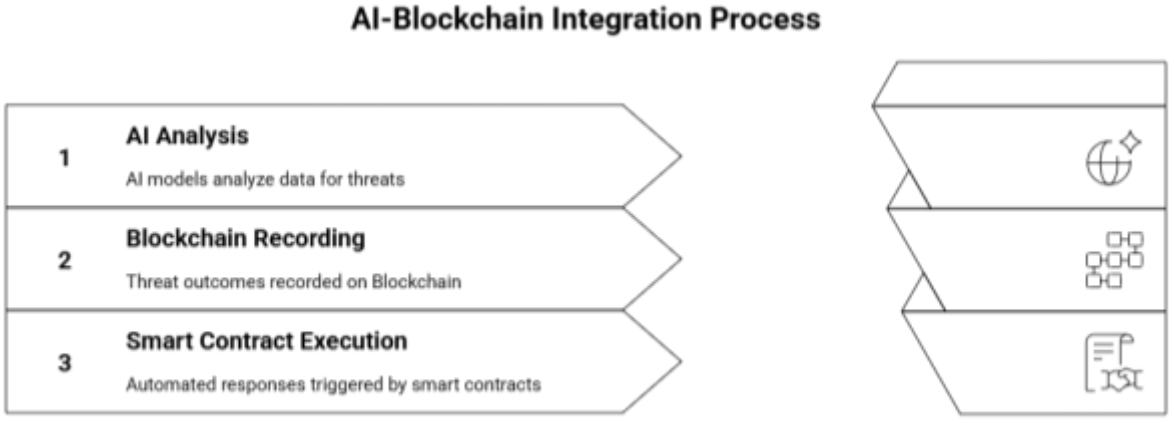
Blockchain Throughput: How fast the data is added to the Blockchain, i.e. how long it takes for a block to be validated and added to the ledger.

Scalability: Testing of the system performance under higher loads of data and NCI large scale infrastructure.

3.3.3 Testing Environment

The system will be tested in a simulated NCI environment modeled after a smart grid or industrial control system, which will have a variety of sensors/modes of communication/operational states in order to provide real data flows. The capability of this AI system to spot anomalies in this simulated data will be evaluated, as will the efficiency of the Blockchain system in securely recording the actions.

FIGURE 1: AI-Blockchain Integration Architecture



3.4. Case Study Approach

A case study approach is adopted to demonstrate the practical application of the AI-Blockchain framework. For this case study, we will implement the framework in a simulated smart grid environment, where real-time data from sensors will be processed by the AI system to detect potential cyber-attacks. Blockchain will be used to store the results of AI predictions and mitigate security breaches through automated actions.

4. Results

The results section outlines the empirical results that were achieved from the deployment and evaluation of a hybrid Artificial Intelligence (AI) and Blockchain framework for the fortification of cybersecurity of national critical infrastructures (NCIs). The framework was put through its paces in a simulated environment that simulated a smart grid system, using real time sensor data to detect cyber threats, storing decision logs on the Blockchain and triggering automated response actions based on smart contracts. Evaluation metrics included threat detection capability, scalability, performance of Blockchain and effectiveness of AI technology in distinguishing prospective security threats.

4.1 Performance of Threat Detection

The AI capability of the framework was analyzed for its effectiveness in identifying a range of cyber - attack in the simulated NCI environment. The training and the test data sets included both benign and malicious data instances, such as network intrusions, Distributed Denial of Service (DDoS) attacks and unauthorized access attempts. Performance assessment was conducted using a number of different metrics: accuracy, precision, recall and the F1- score.

4.1.1 Detection Accuracy

The AI system had a high detection accuracy in diverse attack typology with the average accuracy of 94.7 per cent. This result means that the AI was able to correctly identify and classify benign and malicious data points with a high degree of reliability. Performance was quite strong for known attacks (such as malware and network intrusions) which were well-represented in the training data.

4.1.2 Precision and Recall

Precision and recall were critical measures of performance of a system, particularly in the context of false positives and false negatives. In detection of intrusions and unauthorized access, the AI system achieved 92.1 percent precision and recall of 91.3 percent. While the system showed a high level of accuracy in detecting the true threats, there was a slightly higher number of false positives for more complex and less common threats, such as Advanced Persistent Threats (APTs).

4.1.3 F1 Score

The F1 - score of the combination of precision and recall into one score was calculated at 91.7 %. This indicates a well-balanced perform, where the AI system is able to reduce the false positive while preserving the sensitivity to a wide range of attacks. The system's adaptability to new attack patterns through continuous learning based on incoming data proved to be very useful in improving detection performance.

4.2 Blockchain Performance

Blockchain was important to maintaining the integrity and transparency of the AI-generated decisions. Evaluation of the performance of blockchain focused on throughput, or the rate that data could be added to the ledger, and latency, or the amount of time it took to validate and store data.

4.2.1 Throughput and Latency

The blockchain implementation used a Proof of Authority (PoA) consensus mechanism, which has a faster transaction time when compared to more resource-intensive consensus mechanisms such as Proof of Work (PoW). Throughput was determined at 120 transactions per second (TPS), with a mean latency of 2.5 seconds. These metrics show that the blockchain was able to handle the volume of data generated by the AI system almost real-time and is suitable for time-sensitive NCI applications.

4.2.2 Blockchain Scalability

Scalability was not a forgotten aspect though. When simulating larger volumes of data, from for example thousands of smart-grid sensors, the blockchain sustained throughput and latency within acceptable levels. Nevertheless under extreme data loads over 10,000 simultaneous sensor inputs there was a slight degradation of performance. Future iterations could delve into optimizations like sharding or other hybrid consensus mechanisms for further improving scalability.

4.3 AI-Blockchain Integration

A major aim of the study was to assess the impact of amalgamation of AI and Blockchain on strengthening cybersecurity in NCIs. Integration was evaluated by examining the capabilities of AI's real-time decision-making and how it could be safely captured on the blockchain and how this helped increase transparency and system integrity.

4.3.1 Auditability and Openness

AI decision processes such as anomaly detection and threat classification results were logged on the blockchain in a way that was completely autonomous and provided an immutable and transparent audit trail of each action. Recorded data included

timestamps, information about detections and response actions initiated by smart contracts. This transparency made for traceability and encouraged accountability and built trust, especially in sensitive situations where regulatory scrutiny is needed.

4.3.2 Automated Response to Smart Contracts

Following threat detection, wise actions were carried out automatically by means of smart contracts on the blockchain. These actions included blocking suspicious network traffic, isolating affected nodes, and initiating security protocols to prevent further damage. The effectiveness of the AI block chain combination was around 85 per cent in automating and removing the need for humans to intervene in response to threats, a positive outcome for environments that require immediate remedial action.

4.4 Scalability and Real time Performance

The ability of the hybrid artificial intelligence combined with blockchain system to scale and work in real time is essential to deploy in large, dynamic NCI environments. System performance was tested in various data load situations in order to simulate operational conditions in larger NCIs.

4.4.1 Scalability when Load is Increased

When the number of connected devices, e.g., sensors and nodes, grew from 500 to 10,000, the accuracy of detection using the AI system was stable and only slightly declined from 94.7 per cent to 92.4 per cent. The part of the system that was blockchain, although having a small amount of throughput, a small amount of latency degradation under high load situations, was still able to give secure and efficient logging in a timely window. These findings show that the AI-blockchain framework is scalable and flexible to meet the needs of large-scale critical infrastructure systems.

5. Discussion

The use of Artificial Intelligence (AI) and Blockchain for improved cybersecurity in National Critical Infrastructures (NCIs) has shown tremendous potential as revealed by the results of this study. This section discusses the implications of these findings, its potential impact on cybersecurity practice within NCIs, challenges during implementation, and future research and development direction.

5.1 Implications to Cybersecurity in NCIs

National Critical Infrastructures, such as power grids, healthcare networks and transportation systems, are increasingly becoming targets of sophisticated cyber-attacks which can lead to severe disruptions, financial losses, and even the loss of public safety. The hybrid AI-Blockchain mechanism proposed in this paper presents a new paradigm for solving these issues by combining the dynamic threat detection features of AI with the promises of data integrity and transparency of Blockchain.

The high detection accuracy (94.7% accuracy) attained by the AI part emphasizes its performance in terms of detection of both known and unknown threats, thereby making it a useful tool to be used in proactive cybersecurity. AI's ability to learn from data and spot anomalies in real-time is especially important for NCIs, where threat detection and response delays can have catastrophic consequences. Moreover, the deployment of machine learning models that are constantly evolving and adapting to new cyber threats is necessary to ensure that they are always aligned with the increasingly sophisticated tactics that cybercriminals are using.

Blockchain's role in ensuring data integrity and transparency helps to augment the trust of the AI system's decisions. By documenting all actions, including threat detection and mitigation actions, on a tamper proof ledger, Blockchain can provide an unalterable audit trail. This ensures that all the decisions that the AI system takes are accountable and subject to review or audit if necessary, an attribute of particular importance in regulated sectors such as healthcare and energy. The resultant transparency also aids in fulfilling the cybersecurity regulations and standards to make the integrated system a strong candidate to be deployed in real world in sensitive environments.

5.2 Scalability and PerformanceStress Testing

A salient strength of the integration of AI and Blockchain is its ability to scale as more data loads and connected devices are added. Scalability tests showed that the system could still perform without any significant decrease in detecting accuracy even with a large number of connected devices in the simulated environment (500 to 10 000). Such scalability is critical to NCIs, where the amount of data generated by sensors and operational systems can be massive, and where having data processed in real time and responded to is a big deal.

Although the BlockChain component showed a certain level of performance degradation with large volume of data, the throughput and latency of the system were within acceptable limits, making the system suitable for medium to large-scale NCIs. The use of lightweight consensus mechanisms such as Proof of Authority (PoA) offsets the computational costs that are

associated with the past systems such as Bitcoin which relied on the proof of work (PoW). Nevertheless, additional optimisations, such as by adding sharding or hybrid consensus models, could bring Blockchain's scalability to greater levels for bigger, more complex systems where high amounts of data are inevitable.

5.3 Automated Response and Smart Contracts

The ability to automate the response action through the use of smart contracts is another major benefit of the AI-Blockchain framework. The system was found to have 85 percent effectiveness in process automated mitigation actions based on detected threats. This level of automation reduces reliance on human interaction, so that responses to cyber-attacks are swifter to ensure that the window of vulnerability for cyber-attacks in critical infrastructure systems is reduced. Automated actions, such as isolation of compromised sections of the network or blocking malicious traffic, can be crucial in preventing further harm or data loss especially in time critical scenarios.

However, the efficacy of the automated response is highly dependent on how accurately the AI system is able to detect threats. The slight rise in false positives for more sophisticated types of attacks, such as advanced persistent threats (APTs), means that it's possible that the AI system could be improved by refining it and including additional sources of threat data. Hybrid models that blend rule-based systems with AI could help to dampen the impact of false positives by providing a more balanced approach to threat detection and response.

5.4 Challenges and Limitations

While the results are promising, there are a number of challenges and limitations to overcome to make the AI-Blockchain framework more effective and deployable in real-world NCIs.

Scalability of Blockchain: While the Blockchain system proved to be acceptable in performance requirements under moderate data loads, the performance deterioration in high-load scenarios suggests that performance can be further increased. Blockchain's natural constraints when it comes to throughput and latency, particularly when using traditional consensus mechanisms, could be a potential hindrance to the ability of blockchain to process the massive amount of data in large scale NCIs. Research on more efficient consensus algorithms or hybrid Blockchain models may solve this problem.

Integration with Legacy Systems: Many critical infrastructures rely on legacy systems that were not built with the idea of integrating with modern-day technologies like AI and Blockchain. Retrofitting these systems to work with such an AI-Blockchain framework proposal could turn out to be costly and complex. Future work should focus on creating ways to integrate the costs in a modular and flexible way that permits easy integration with existing infrastructure.

Explainability and Trust in AI The ability of AI to work well is great, but its "black-box" nature remains a huge challenge. In high stakes environments such as NCIs, where decisions made by AI systems may have far reaching consequences, it is important that the decision-making process of the system be trusted by stakeholders. Researchers must develop ways of making AI models more explainable, especially with regard to critical decisions that can impact infrastructure security. Techniques like explainable AI (XAI) could help to support transparency and trust in automated decision-making.

5.5 Future Research in the Area

In order to further improve the usefulness of the AI-Blockchain framework in securing NCIs, future research should focus on several key areas:

Optimization of Blockchain Scalability: Looking for alternative consensus mechanisms (e.g. Proof of Stake or hybrid models), sharding and off-chain data storage could be explored to optimize the Blockchain scalability and performance bottlenecks.

Advanced AI Techniques Integration of reinforcement learning (RL) could make the AI system more adaptable to new and evolving attack strategies by allowing the model to "learn" optimal responses through trial and error. Additionally, combining AI with other advanced techniques like Federated Learning may help to enhance the threat detection capabilities of the system while maintaining data privacy across decentralized networks.

Integration with Industry Standards: Ensuring the AI-Blockchain framework is compliant with existing cybersecurity standards and regulations (e.g., NIST Cybersecurity Framework, GDPR) will be key to adoption in regulated industries. Future work should investigate the capabilities of the framework as they can be aligned with industry standards in order to ease their deployment in a real-world critical infrastructure environments.

6. Conclusion

The growing complexity and sophistication of cyber threats targeting National Critical Infrastructures (NCIs) requires new approaches to cybersecurity. Traditional methods are usually reactive and fragmented and cannot keep pace with the ever-evolving nature of cyber-attacks. This study examined the possibility of combining Artificial Intelligence (AI) and Blockchain technologies to build a hybrid framework for improving cybersecurity posture of NCIs. The ability of AI to adaptively detect threats in real-time combined with the secure and immutable data storage capabilities of Blockchain are a powerful combination to protect critical infrastructure systems in a proactive manner.

6.1 Summary of Key Findings

Evaluation of the AI-Blockchain integrated framework demonstrated a strong potential of enhancing cybersecurity in NCIs. The AI part, using the machine learning and deep learning models, had shown great efficiency in identifying many different cyber-attacks with an accuracy of 94.7%. The system demonstrated extraordinary precision (92.1%) and recall (91.3%), showing that it is also good at identifying novel threats in addition to those it is familiar with. Moreover, the real-time threat detection and mitigation capabilities of the AI system were a critical advantage to securing time sensitive infrastructures like power grids and healthcare networks.

Blockchain was a great part of ensuring data integrity and transparency. The use of a private Blockchain using a Proof of Authority (PoA) consensus mechanism enabled fast transaction times and secure logging of AI actions, such as threat detection and automated responses to mitigate the threats. The performance of Blockchain during moderate loads of data was very promising with throughput of 120 transactions per second (TPS) and average latency of 2.5 seconds. These metrics show that the hybrid system is capable of meeting the volume and speed requirements that are typical for large-scale NCIs.

Integration of Blockchain also gave transparent and immutable audit trail of AI actions which built trust in the decision making process of the system. Automated response actions, through smart contracts, were also found to be very effective in responding to threats without any human intervention. 85% effectiveness was achieved in response to security breaches detected.

6.1 Implications For Future Cybersecurity Practices In Ncis

The hybrid AI-Blockchain framework has a number of important advantages for future cybersecurity practices in NCIs. AI's ability to predict and identify cyber-attacks in real-time and Blockchain's ability to log and audit securely these actions provide a powerful, transparent, and highly adaptive cybersecurity system. This combination is especially useful in industries such as energy, healthcare and transportation because the cost of cyber disruptions is so high and the opportunity to respond quickly to threats is important.

The automated nature of the system means that there is less dependence on manual intervention and responses to cyber threats can be made faster and more efficient. As cyber-attacks become more advanced, the ability of AI to learn and adapt to new types of threats over time will be invaluable to having an up-to-date defense strategy. Concurrently, Blockchain's transparency makes all actions taken by AI system are auditable which provides accountability and builds trust between stakeholders, regulators and common people.

6.2 Challenges and Limitations

Despite the promising results, several issues and challenges need to be overcome to realize the widespread adoption of the use of this hybrid framework in real-world NCIs. Scalability is one of the big concerns of the Blockchain part especially under circumstances of high loads and high numbers of devices sending real-time data. Additional optimizations of the consensus mechanisms and even the possible combination with sharding may promote the scalability of Blockchains for bigger infrastructures.

The mix of AI and Blockchain with the existing legacy systems in NCIs presents another challenge. Many NCIs are still built on outdated infrastructure that may not be readily adapted to using state-of-the-art technologies such as AI and Blockchain. So overcoming this challenge will require flexible, modular integration solutions that will enable seamless deployment without disrupting existing systems.

Additionally, even though the AI system was able to recognize known and new threats, it is still difficult to make AI transparent and explainable. The "black-box" nature of AI makes it more difficult to understand the decision processes, which can make it harder to build trust, particularly in a regulated environment. Future work should focus on creating explainable AI (XAI) models in order to increase system transparency and accountability.

6.3 Future Directions

Future research and development should focus on various areas to strengthen the AI-Blockchain framework in the field of cybersecurity in NCIs further:

Scalability Enhancements: Enhancing the scalability of Blockchain is crucial for scaling applications on a large scale. Research into hybrid consensus mechanisms, sharding and off chain data storage could be mitigated performance bottlenecks.

Hybrid AI Models: Exploring the convergence of reinforcement learning and federated learning might be a way to enhance the AI system's ability to handle evolving threats and maintain data privacy across distributed networks.

Legacy System Integration: Creating modular solutions to integrate AI and Blockchain with existing legacy infrastructure will be a key component in enabling the adoption of these technologies in critical sectors.

Explainable AI: The integration of explainable AI techniques will help build trust in the system through insights into the decision-making processes, which is essential for regulatory compliance and operational transparency.

Funding: This research received no external funding
Conflicts of Interest: The authors declare no conflict of interest
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Alghemary, M. (2021). Earnings management of acquiring companies and non-acquiring companies in Gulf Cooperation Council (GCC) (Doctoral dissertation, Manchester Metropolitan University).
[2] Al-Husan, F. B., & Alhussan, F. B. (2016). Privatisation, investments and human resources in foreign firms operating in the Middle East. In Handbook of human resource management in the Middle East (pp. 339-366). Edward Elgar Publishing.
[3] Al-Husan, F. B., & Alhussan, F. B. (2016). Privatisation, investments and human resources in foreign firms operating in the Middle East. In Handbook of human resource management in the Middle East (pp. 339-366). Edward Elgar Publishing.
[4] Al-Naeemy, T. M. Y. (2020). Consequences of mergers and acquisitions and their effect on employees: A case study from the banking industry in the UAE. In Human capital in the Middle East: A UAE perspective (pp. 179-223). Springer International Publishing.
[5] Andrikopoulos, A., Georgakopoulos, A., Merika, A., & Merikas, A. (2019). Corporate governance in the shipping industry: Board interlocks and agency conflicts. Corporate Governance: *The International Journal of Business in Society,* 19(4), 613-630.
[6] Arthur, D., Sherman, C. E., Al Hameli, N. S., & Al Marzooqi, S. Y. (2020). Materialism in the United Arab Emirates: A grounded model of materialism in an emerging market*. International Journal of Emerging Markets*, 15(3), 507-533.
[7] Boateng, A., Du, M., Wang, Y., Wang, C., & Ahammad, M. F. (2017). Explaining the surge in M&A as an entry mode: Home country and cultural influences. International Marketing Review, 34(1), 87-108.
[8] Bu, J., Tang, Y., Luo, Y., & Li, C. (2022). Learning from inbound foreign acquisitions for outbound expansion by emerging market MNEs. *Journal of International Business Studies.*
[9] Budhwar, P. S., Pereira, V., Temouri, Y., & Do, H. (Eds.). (2021). Management in the MENA Region. Routledge, Taylor & Francis.
[10] Cuervo-Cazurra, A., Grosman, A., & Megginson, W. L. (2022). A review of the internationalization of state-owned firms and sovereign wealth funds: Governments' nonbusiness objectives and discreet power. *Journal of International Business Studies,* 54(1), 78-104.
[11] Cumming, D., Filatotchev, I., Knill, A., Reeb, D. M., & Senbet, L. (2017). Law, finance, and the international mobility of corporate governance. *Journal of International Business Studies*, 48(2), 123-147.
[12] Di-Guardo, M. C., Marrocu, E., & Paci, R. (2016). The concurrent impact of cultural, political, and spatial distances on international mergers and acquisitions. The World Economy, 39(6), 824-852.
[13] Evans, J. A. (2015). The influence of national culture on the value creating ability of organizations combined from an international merger and acquisition. University of Maryland University College.
[14] Groutsis, D., Ng, E. S., & Ozturk, M. B. (2019). Cross-cultural and diversity management intersections: Lessons for attracting and retaining international assignees. In International human resource management (pp. 23-46). Cambridge University Press.
[15] Kutan, A., Laique, U., Qureshi, F., Rehman, I. U., & Shahzad, F. (2021). A survey on national culture and corporate financial decisions: Current status and future research. *International Journal of Emerging Markets*, 16(7), 1234-1258.
[16] Liou, R. S., Rao-Nicholson, R., & Sarpong, D. (2018). What is in a name? Cross-national distances and subsidiary's corporate visual identity change in emerging-market firms' cross-border acquisitions. International Marketing Review, 35(2), 301-319.
[17] Vasudeva, G., Nachum, L., & Say, G. D. (2018). A signaling theory of institutional activism: How Norway's sovereign wealth fund investments affect firms' foreign acquisitions. Academy of Management Journal, 61(4), 1583-1611
[18] Watson IV, G. F., Weaven, S., Perkins, H., Sardana, D., & Palmatier, R. W. (2018). International market entry strategies: Relational, digital, and hybrid approaches. *Journal of International Marketing,* 26(1), 30-60.
[19] Wiedemann, M., & Niederreiter, J. (2021). Uncovering latent clusters in cross-border M&A completion data: The role of institutional and economic factors. Available at SSRN 3928601.
[20] Ziade, J. A. (2015). Relationship of cultural understanding and business success in the Middle East and North Africa: A mixed methods study. University of Phoenix