e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AI Cyber Chain- Combining AI and Blockchain for Improved Cybersecurity

Shobha Agasibagil, Harsha D U, Abhishek Simha M

Assistant Professor, Department of Computer Science Engineering, Channabasaveshwara Institute of Technology, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science Engineering, Channabasaveshwara Institute of Technology, Tumkur, Karnataka, India

U.G. Student, Department of Computer Science Engineering, Channabasaveshwara Institute of Technology, Tumkur, Karnataka, India

ABSTRACT: One of the major technologies of the Industrial Revolution that has the potential to defend against cybersecurity threats is artificial intelligence (AI). AI makes precise real-time data analysis possible and is a crucial part of big data analytics. AI is capable of analysing large amounts of data, yet it has limitations with regard to data centralization, security, and privacy. As cybercriminals continue to develop, law enforcement is facing increasing challenges. It is more difficult to identify and prevent complex cyberattacks with conventional cybersecurity technologies.

I. INTRODUCTION

Two quickly evolving areas that are anticipated to have a big influence on cybersecurity are artificial intelligence (AI) and blockchain technology. AI has the potential to automate danger identification and real-time response. Algorithms for machine learning can be trained to detect known and zero-day threats as well as patterns of hostile activity. One notable technology that has been receiving a lot of interest from academics and industry is artificial intelligence. With the ongoing rise in cyberthreats in AI.

The integration of AI, cybersecurity, and blockchain is an emerging field with the potential to revolutionize digital security. Traditional cybersecurity methods often struggle to keep up with the rapidly evolving and complex nature of modern cyber threats. AI has become a crucial asset in cybersecurity due to its capacity to analyse large volumes of data, identify anomalies, and react to threats in real-time. However, many AI systems are centralized, which makes them attractive targets for cyber-attacks.

Blockchain technology offers a promising way to address these vulnerabilities. With its decentralized, transparent, and immutable structure, blockchain distributes data across a network of nodes, eliminating single points of failure and strengthening the integrity and authenticity of data. This makes blockchain an ideal partner for AI in enhancing cybersecurity.

This solution can produce a transparent, distributed, traceable, and immutable audit trail. As a result, blockchain offers several advantages that could significantly contribute to solving cybersecurity challenges. Integrating AI and blockchain in cybersecurity has the potential to develop innovative solutions that strengthen the overall security framework of organizations. One strategy involves deploying decentralized AI models on a blockchain network, ensuring secure and transparent handling of sensitive data while maintaining a tamper-proof system.

In this paper, we introduce the AICyber-Chain model, a solution that combines AI and blockchain to tackle current cybersecurity challenges. Our model leverages the strengths of both AI and blockchain to overcome the limitations of traditional cybersecurity approaches, offering a robust and comprehensive solution for enhancing data security.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. RELATED WORK

This section reviews the literature on safe data transfer and data exchange, paying particular emphasis to the combination of blockchain technology with artificial intelligence. The advent of technologies such as artificial intelligence (AI) and blockchain has created new opportunities and opened up new paths for cybersecurity research, development, and application.

In many aspects, artificial intelligence (AI) is better than other technologies in cyberspace [1]. Machine learning and artificial intelligence (AI) can help track down hackers, automate threat detection, and identify threats faster and more precisely than traditional software or human intervention, especially when cyberattacks and device proliferation rise dramatically [15]. AI-based cyberattacks are now far more common among hackers. In order to fool AI-based cybersecurity, which is taught to recognize and exploit weaknesses, hackers need to hackers must first target classification algorithms.

A. SHARING SECURE DATA

The application of blockchain technology for safe data sharing has been the subject of numerous research. A blockchain-based architecture for safe and open data sharing in the medical field was put up by Xu et al. [16]. Their method guarantees traceability and data integrity, both of which are essential for sensitive health data.

B. TRANSMITTING DATA SECURELY

Another crucial element that has been improved by the combination of blockchain and AI is secure data transmission. A blockchain-based solution was created by Nair et al. [5] to protect data transfer in Internet of Things networks. Their technology lowers the danger of data breaches by using smart contracts to automate and enforce security regulations during data transmission. Secure data transfer is another area where AI approaches have been used.

C. APPLYING BLOCKCHAIN AND AI TO SECURE DATA OPERATIONS

In recent years, there has been an increase in interest in the use of blockchain technology in conjunction with artificial intelligence for safe data processing. According to Khademi and Honavar [19], blockchain guarantees the integrity and immutability of the events that are noticed, while artificial intelligence (AI) can be utilized to identify irregularities and possible threats in real-time. A more secure environment for data operations is produced by this synergy.

D. THE RISKS OF AI AND SECURITY IN CLOUD COMPUTING

Since AI algorithms need to use vast volumes of data from as many sources as possible, data security is a critical issue for all network designs and serves as the basis for their advancement. Additionally, an improved AI will be able to recognize a wider range of threats, enhancing security even more at a higher level

III. PROPOSED WORK

The suggested AICyber-Chain system is a cybersecurity framework that combines blockchain technology and artificial intelligence (AI) to improve the dependability and security of digital environments. The technology uses artificial intelligence's sophisticated anomaly detection, threat prediction, and pattern recognition skills to instantly spot possible cyberthreats. In order to identify vulnerabilities and highlight malicious activity, machine learning models continuously examine user behaviour, network traffic, and system anomalies.

Blockchain serves as a decentralized, impenetrable record for safely keeping private information including threat intelligence, AI model settings, and security logs. Because of its distributed architecture, which eliminates single points of failure and makes it nearly impossible for cybercriminals to change data, it guarantees data openness and integrity. Smart contracts can provide a quick and efficient solution by automating reactions to threats that are discovered. And reliable countermeasure against attacks.

AICyber-Chain provides a multi-layered security strategy by fusing the predictive capabilities of AI with the safe data handling capabilities of Blockchain. This integrated system offers a strong defense against advanced cyberattacks and is made to change and react when new threats appear. By guaranteeing the confidentiality, integrity, and accessibility

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

of vital assets for businesses and users, AI Cyber-Chain seeks to promote a safe, open, and effective digital environment.

IV. SYSTEM MODEL

The Peer-to-peer communication is crucial to the establishment of a shared IPFS structure in our suggested AICyber-Chain paradigm (FIGURE 2). consensus based on the blockchain concept. The nodes exchange information with each other through smart contracts.

Blockchain ledgers that synchronize the state with peer nodes are used to execute smart contracts. The AICyber-Chain architecture offers a strong and safe foundation for data operations by combining blockchain technology with AI-driven cybersecurity measures. The main concept is to use AI real-time threat detection, adaptive security measures, and blockchain's decentralized ledger and immutability properties.

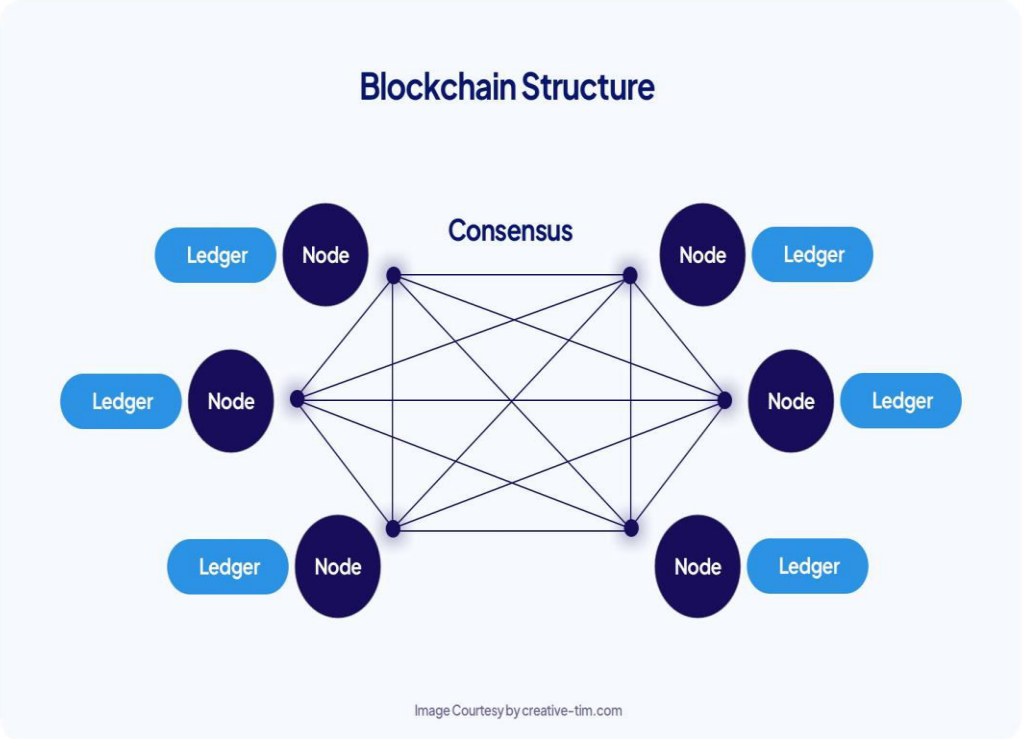

FIGURE 1. Structure of Blockchain.

1) Since blockchain data is not kept in a single central database, it is protected from manipulation. There is just one compromised copy of the blockchain when a security system is broken or stolen.

2) Immutability: Blockchain technology is used to maintain distributed ledgers internationally. Any change to the block contents without the majority's approval is prevented by synchronized ledgers.

3) Consensus and Trust: By offering fault-tolerant consensus procedures (solving mechanisms), distributed processes and multi-agent systems, like cryptocurrencies, produce a single value.

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

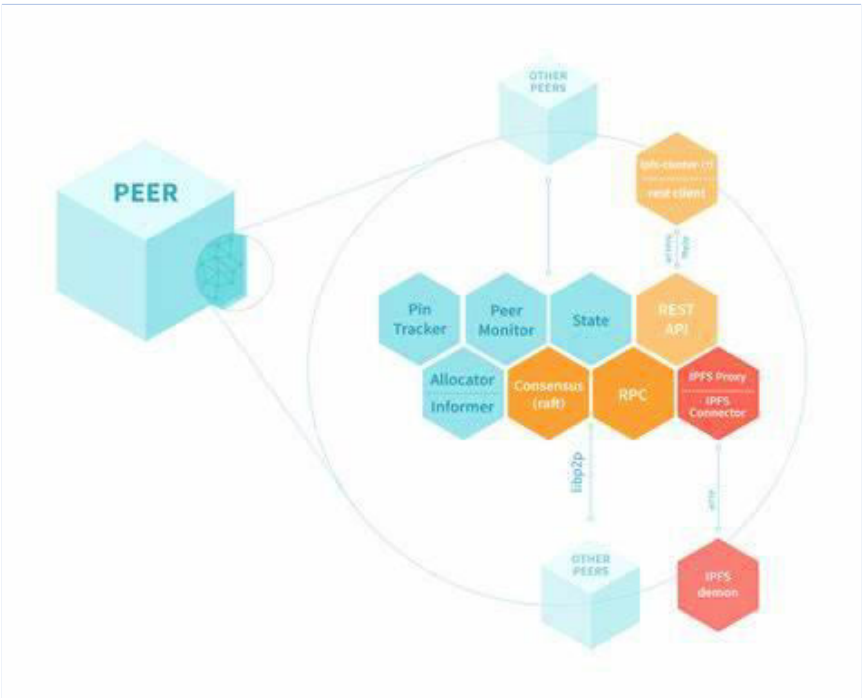

FIGURE 2. IPFS structure.

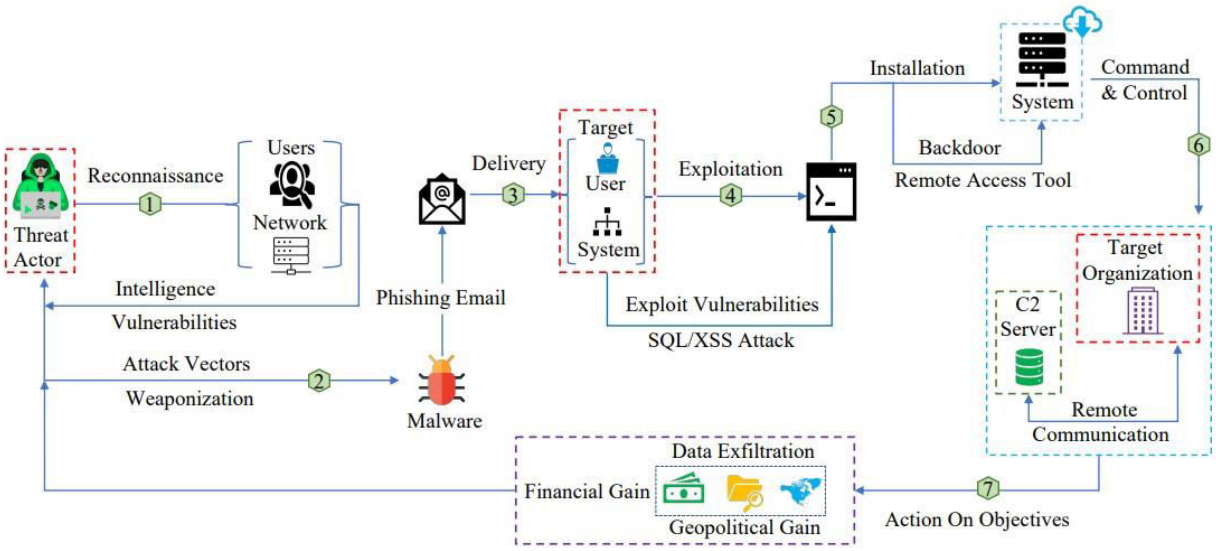

FIGURE 3. Proposed AICyber-Chain model.

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

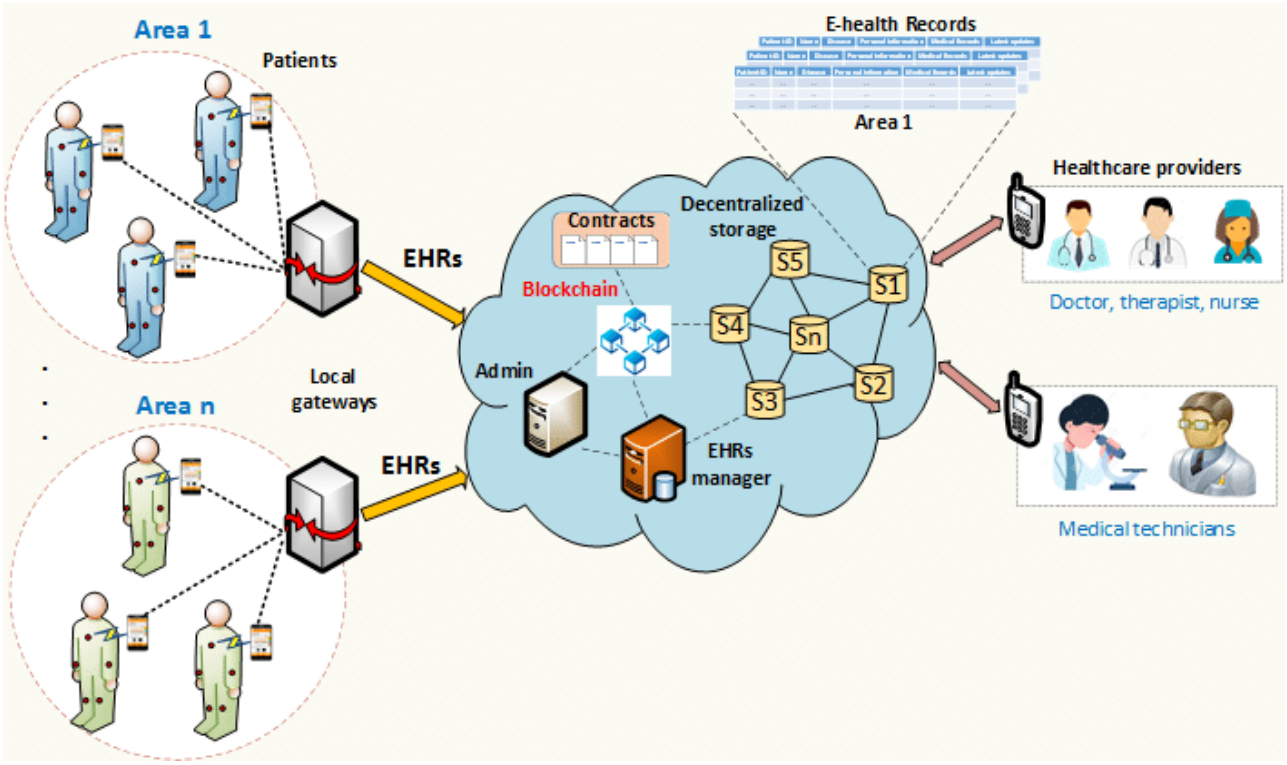

FIGURE 4. PROPOSED AICYBER-CHAIN IN MEDICAL DATA SHARING.

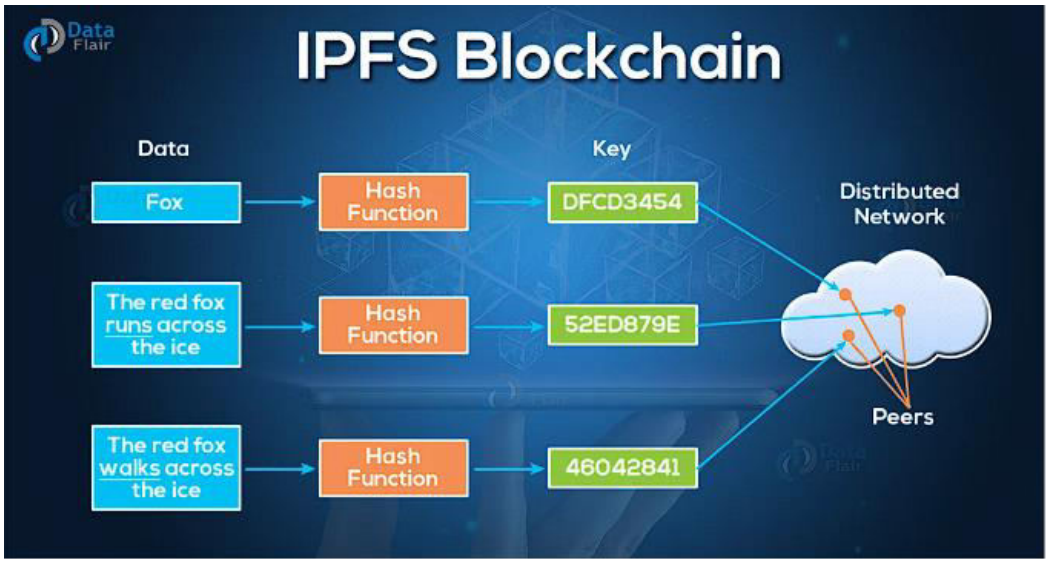

FIGURE 5. IPFS-based data storage using blockchain technology.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

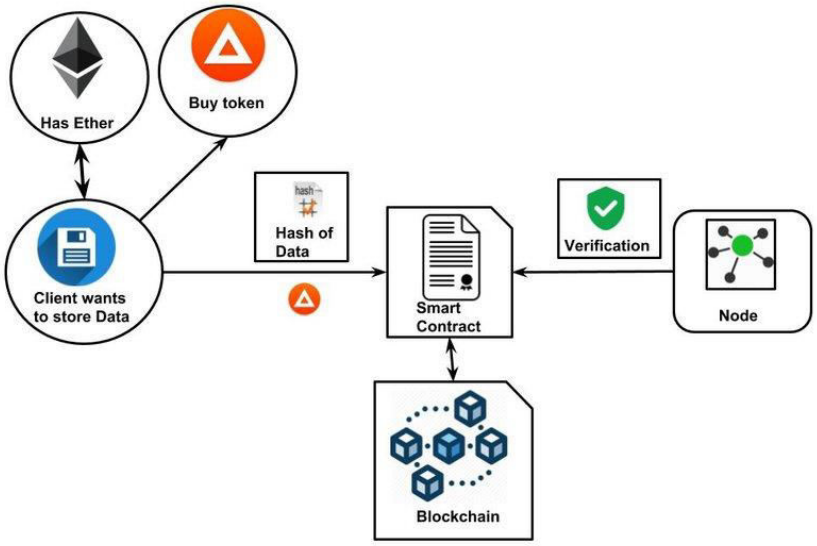

FIGURE 6. Proposed AICyber-Chain smart contract workflow.

V. USE CASE SCENARIO

Because AI and blockchain are inherently integrated, AICyber-Chain will be able to facilitate a wide range of applications. The creation and deployment of AICyber-Chain applications is frequently employed in scenarios where the confidentiality and integrity of medical data are ensured by a network of accountable parties. Creating a cutting-edge, safe, and accessible healthcare data management environment is the aim. Experimental data, interpretations, and conclusions are succinctly and accurately described.

VI. CONCLUSION AND FUTURE WORK

The increasing demand for more sophisticated and secure techniques to safeguard sensitive data has led to a rise in the use of AI and blockchain technology in cybersecurity. In contrast, blockchain provides a decentralized, safe platform for information sharing and storage. It guarantees the integrity and validity of transactions and aids in preventing unwanted access to data with its immutable ledger and cryptographic methods. Organizations can improve their entire security posture and defend against a greater variety of cyberthreats by integrating the advantages of these two technologies.

In this research, we have introduced a novel method that combines blockchain-based adaptive smart contract execution with AI-driven threat detection. The system's excellent detection accuracy, quick response time, and useful adaptability are demonstrated by the performance evaluation, highlighting its potential to improve cybersecurity in dynamic contexts.

Blockchain and artificial intelligence (AI) have the potential to significantly improve cybersecurity initiatives. Both blockchain technology and artificial intelligence (AI) provide special advantages that can be used to strengthen defences against online threats. AI can be applied to data protection, network security, threat intelligence, and fraud detection.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

[1] R. Salama, F. Al-Turjman, C. Altrjman, S. Kumar, and P. Chaudhary, ''A comprehensive survey of blockchain powered cybersecurity—A survey,'' in Proc. Int. Conf. Compute. Intel., Commun. Technol. Netw. (CICTN), Apr. 2023, pp. 774–777.

[2] Y. A. Kadakia, A. Suryavanshi, A. Alnajdi, F. Abdullah, and P. D. Christofides, ''Integrating machine learning detection and encrypted control for enhanced cybersecurity of nonlinear processes,'' Compute. Chem. Eng., vol. 180, Jan. 2024, Art. no. 108498.

[3] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, ''Weaponized AI for cyber-attacks,'' J. Inf. Secure. Appl., vol. 57, Mar. 2021, Art. no. 102722.

[4] J. Ahmad, M. U. Zia, I. H. Naqvi, J. N. Chattha, F. A. Butt, T. Huang, and W. Xiang, ''Machine learning and blockchain technologies for cybersecurity in connected vehicles,'' WIREs Data Mining Knowl. Discovery, vol. 14, no. 1, p. e1515, Jan. 2024.

[5] M. M. Nair, A. Deshmukh, and A. K. Tyagi, ''Artificial intelligence for cyber security: Current trends and future challenges,'' in Automated Secure Computing for Next-Generation Systems. Hoboken, NJ, USA: Wiley, 2024, pp. 83–114.

[6] In "Introduction: Cyberspace, Cyberterrorism, and the International Security in the Fourth Industrial Revolution: Threats, Assessment, and Responses," R. Montasari discusses the threats, assessments, and reactions related to cyberspace, cyberterrorism, and international security in the fourth industrial revolution.

[7] R. Yan, "Chitty-chitty-chat bot: Deep learning for conversational AI," in Proceedings of the International Journal on Conversational AI, vol. 18, 2018, pp. 5520–5526.

[8] "A causal perspective on algorithmic bias in recidivism prediction" (student abstract) by A. Khademi and V. Honavar, in Proc. AAAI Conf. Artif. Intell., 2020, vol. 34, no. 10, pp. 13839–13840.

[9] Artificial Intelligence in Times of Turbulence: Theoretical Foundation to Applications, by T. Sharma and P. 81–98, Hershey, PA, USA.

[10] In Big Breaches, N. Daswani and M. Elbayadi discuss "Facebook security issues and the 2016 US presidential election." Springer, Berlin, Germany, 2016, pp. 97–130.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com