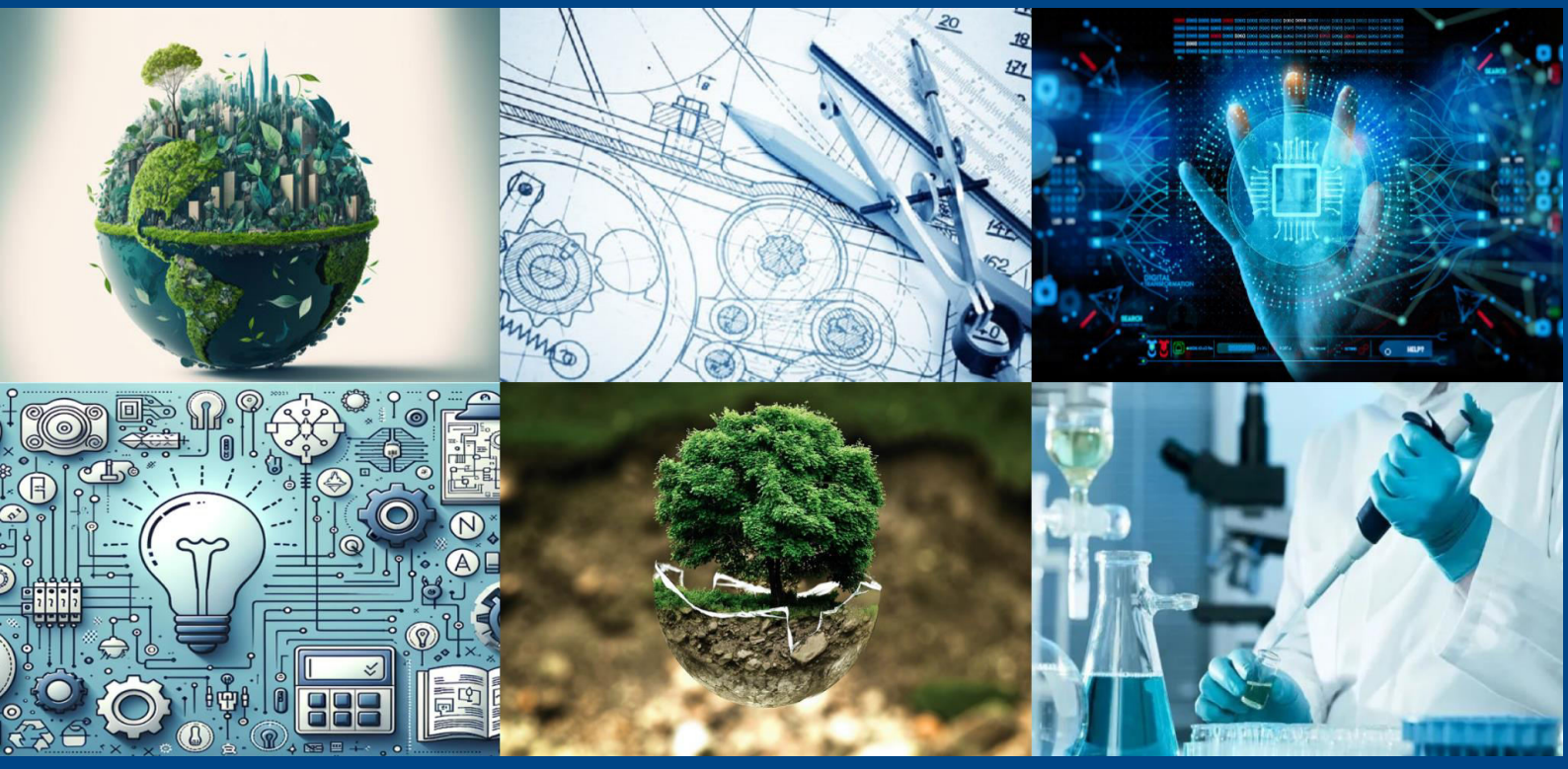
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 8, Issue 3, March 2025**

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803263

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

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

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

Securing Cyber-Physical System with Blockchain Backed Attack Detection

DR.D.J. Samatha Naidu, K. Venkata Ramya, M. Priyanka

Professor, Dept. of MCA APGCCS, New Boyanapalli, Rajampet, AP, India

Assistant Professor, Dept. of MCA APGCCS, New Boyanapalli, Rajampet, AP, India

PG Student, Dept. of MCA APGCCS, New Boyanapalli, Rajampet, AP, India

ABSTRACT: Cybersecurity challenges pose a significant threat to Healthcare Cyber-Physical Systems (CPS), which heavily rely on wireless communication. Jamming attacks can severely disrupt the integrity of these networks, leading to compromised performance and security risks. To address this issue, a decentralized system is introduced that leverages trust mechanisms and blockchain technology to enhance security against jamming threats. A layered model is designed to improve network lifetime and overall system performance in smart healthcare environments. This approach ensures secure and reliable communication between sensor nodes, wearable sensors, medical devices, and monitoring systems, thereby strengthening the resilience of healthcare CPS against cyber threats. By integrating a trust-based framework with blockchain, data authenticity and transparency are significantly enhanced. The proposed model also reduces reliance on centralized security solutions, mitigating single points of failure. This contributes to the advancement of secure and efficient healthcare CPS by addressing key vulnerabilities in wireless network communication.

I. INTRODUCTION

The increasing reliance on Cyber-Physical Systems (CPS) in various sectors, particularly in healthcare, has brought about significant advancements in technology and efficiency. However, these systems are increasingly vulnerable to cybersecurity threats, especially those targeting wireless communication channels. Among the various cyberattacks, jamming poses a particularly serious risk to the integrity and functionality of CPS networks. These attacks disrupt communication between devices, compromising the accuracy and reliability of the entire system.

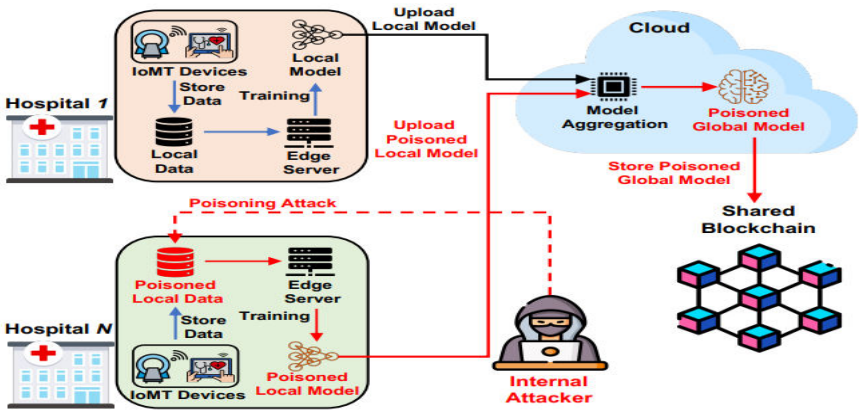


Figure 1: CPS & Blockchain Architecture

Blockchain technology, known for its decentralized and tamper-proof nature, has emerged as a promising solution for enhancing the security of CPS. By leveraging blockchain's capabilities, it is possible to detect and mitigate attacks such as jamming more effectively. This paper explores the potential of using blockchain to support a robust assault detection mechanism in CPS, aiming to create a system that not only identifies threats but also prevents them from severely

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

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

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

affecting the performance of critical networks. The proposed system combines trust mechanisms and blockchain technology to provide real-time monitoring and response to security breaches, ensuring that healthcare CPS networks remain operational and secure. Through the use of a layered model, the system also aims to improve the overall lifetime and efficiency of these networks, ensuring reliable communication between sensor nodes, medical devices, and monitoring systems.

II. LITERATURE REVIEW

[1] G. Mohler, ``Marked point process hotspot maps for homicide and gun crime [1] Natalia A. Popova, Natalia G. Butakova " Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transact ions",‖ 978-1-7281-0339-6/19/$31.00 ©2019 IEEE

This paper discusses the use of Blockchain technology without tokens to protect information about banking transactions, namely, transfer amounts, card details, names of participants, etc. This topic is relevant, since the digital economy is becoming an integral part of modern life. The processed information passes through the database of banks and payment systems, which potentially makes it available to the attacker. The article analyzes the protection mechanisms of distributed databases, proposes a solution to the problem of maintaining the uniqueness of information in them based on Blockchain technology without tokens and gives recommendations on the introduction of Blockchain technology into modern banking systems.

[2] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3 " An Overview of Blockchain Technology: Archit ect ure, Consensus, and Fut ure Trends" 2017 IEEE 6th International Congress on Big Data

Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architechture firstly and compare some typical consensus algorithms used in different blockchains. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future trends for blockchain.

[3] Pasu Poonpakdee∗, Jarotwan Koiwanit ∗, Chumpol Yuangyai∗ and Wat chara Chatwiriya" Applying Epidemic Algorithm for Financial Service based on Blockchain Technology" 978-1-5386-4956- 5/18/$31.00 ©2018 IEEE.

Our global market is emerging transformation strat-egy that can make the difference between success and failure.Smart contract systems through developments of technologicalinnovations are increasingly seen as alternative technologies toimpact transactional processes significantly. Blockchain is a smartcontract protocol with trust offering the potential for creatingnew transaction platforms and thus shows a radical change ofthe current core value creation in third parties. These resultsin enormous cost and time savings and the reduced risk for theparties. This study proposed a method to improve the efficiency ofdistributed consensus in blockchains using epidemic algorithm.The results showed that epidemic protocols can distribute theinformation similar to blockchain.

[4] Satoshi Nakamoto "‖ Bitcoin: A Peer-to-Peer Elect ronic Cash System"

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803263

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

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

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

Relevance to current Research

Blockchain technology has been known as a cryptocurrency platform since the emergence of its first and largest application, bitcoin. Blockchain contributes to the process of changing low-trust centralized transaction ledger held by a single third party, to high-trust decentralized form held by different verifying nodes. Due to its decentralized nature and security robustness, blockchain has big potentials to be applied in various fields beyond cryptocurrency. This paper aims to provide readers a more complete literature review of blockchain, compared with existing works. We introduce and explain various security properties of blockchain, provide a taxonomy of blockchain-based applications, and discuss challenges of blockchain in terms of security and performance. Furthermore, some research directions are given in the last section of the paper.

III. METHODOLOGY OF PROPOSED SURVEY

The proposed system integrates attack detection, trust evaluation, and blockchain storage to enhance security in Cyber-Physical Systems (CPS). Below are the key algorithms used in the system to detect cyber threats and securely store attack logs.

1. Hybrid Trust-Based Attack Detection Algorithm

This algorithm evaluates device behavior and historical reputation to detect cyber-attacks in CPS networks.
Steps of the Algorithm:

1. Input: Security log L from CPS device D.
2. Extract features (e.g., packet loss, unauthorized access, abnormal traffic patterns).
3. Calculate Reputation Trust (RT) using past behavior logs:

RT(D) = \frac{\text{Successful transactions}}{\text{Total transactions}}
BT(D) = 1 - \frac{\text{Anomalous events}}{\text{Total events}}
FTS(D) = \alpha \cdot RT(D) + (1 - \alpha) \cdot BT(D)

6. If FTS(D) < Threshold, classify D as a malicious device and log the event.
7. Else, classify D as a normal device.
8. Output: Attack detection result stored in security logs.

2. Blockchain-Based Security Log Storage Algorithm

Once an attack is detected, this algorithm stores the log in the blockchain for tamper-proof security.
Steps of the Algorithm:

1. Input: Security Log L = {Attack_ID, Device_ID, Timestamp, Attack_Type}.
2. Generate Hash H(L) using SHA-256 hashing:

H(L) = \text{SHA-256}(L)

4. Execute a smart contract to verify and store the transaction.
5. If blockchain consensus is reached, store the block permanently.
6. Output: Security log is stored in the blockchain, ensuring immutability.

3. Smart Contract-Based Automatic Response Algorithm

This algorithm automates security responses based on attack severity.
Steps of the Algorithm:

1. Input: Attack Log A = {Attack_Type, Severity_Level, Device_ID}.
2. Define action rules in a smart contract (e.g., block IP, alert admin, log event).
3. If Severity_Level > High, execute BLOCK_DEVICE(Device_ID).
4. Else if Severity_Level = Medium, send an alert to the admin.
5. Else, log the event in blockchain for review.
6. Output: Automated security response is triggered.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

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

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

IV. CONCLUSION AND FUTURE WORK

In this paper, introduces a hybrid trust model that includes blockchain technology and smart contracts to find possibilities for jamming attacks across CPS networks. The proposed framework shall deploy a unique set of trust assessment techniques, rather than on the reputation and behavior of the nodes, to warrant an accurate and intensive evaluation of the latter's reliability In addition, smart contracts, systems, sensor nodes, and fog nodes. Smart contracts automatize and secure the registration process to assure all network entities that the records are safe and transparent. The proposed integrated approach, while ensuring scalability and flexibility, provides a resilient way to protect CPS networks from jamming attacks. This method allows for real-time response and continuously improves the network's security. Further, the design addressed the requirements concerning the technology devices that can guarantee reliable and secure communication in the healthcare environment, such as the Internet of Things. In future, we aim to expand the suggested method and evaluating its effectiveness across real life healthcare test-bed and network configurations. Additionally, we also aim to use cutting-edge AI and ML techniques to increase the trust evaluation process to identify a wide range of other attacks. As technology advances and cyber threats become more sophisticated, the Blockchain-Backed Assault Detection System for Cyber-Physical Systems (CPS) can be further improved to provide better security, efficiency, and scalability. While the current system effectively detects and records cyber-attacks using blockchain, there are several ways it can be enhanced in the future to adapt to evolving cybersecurity challenges. While the Blockchain-Backed Assault Detection System for Cyber-Physical Systems (CPS) already provides a secure, decentralized, and efficient approach to cybersecurity, several enhancements can further improve its accuracy, scalability, and adaptability.

REFERENCES

[1] A. Mishra, A. V. Jha, B. Appasani, A. K. Ray, D. K. Gupta, and A. N. Ghazali, ''Emerging technologies and design aspects of next generation cyber physical system with a smart city application perspective,''Int. J. Syst. Assurance Eng. Manage., vol. 14, no. S3, pp. 699–721, Jul. 2023.

[2] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, and A. Derhab, ''A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in Internet of Things,'' Sensors, vol. 21, no. 1, p. 23,Dec. 2020.

[3] B. A. Salau, A. Rawal, and D. B. Rawat, ''Recent advances in artificial intelligence for wireless Internet of Things and cyber–physical systems. A comprehensive survey,'' IEEE Internet Things J., vol. 9, no. 15, pp. 12916–12930, Aug. 2022.

[4] S. A. Moqurrab, A. Anjum, N. Tariq, and G. Srivastava, ''An efficient framework for semantically-correlated term detection and sanitization in clinical documents,'' Comput. Electr. Eng., vol. 100, May 2022, Art. no. 107985.

[5] D. Patel, C. K. Sahu, and R. Rai, ''Security in modern manufacturing systems: Integrating blockchain in artificial intelligence-assisted manufacturing,'' Int. J. Prod. Res., vol. 62, no. 3, pp. 1041–1071, Feb. 2024.

[6] M. Hammoudeh, G. Epiphaniou, and P. Pinto, ''Cyber-physical systems: Security threats and countermeasures,'' J. Sensor Actuator Netw., vol. 12, no. 1, p. 18, Feb. 2023.

[7] W. Li, Y. Chai, F. Khan, S. R. U. Jan, S. Verma, V. G. Menon, F. Kavita, and X. Li, ''A comprehensive survey on machine learning-based big dataanalytics for IoT-enabled smart healthcare system,'' Mobile Netw. Appl., vol. 26, no. 1, pp. 234–252, Feb. 2021.

[8] L. Javed, A. Anjum, B. M. Yakubu, M. Iqbal, S. A. Moqurrab, and G. Srivastava, ''ShareChain: Blockchain-enabled model for sharing patientdata using federated learning and differential privacy,'' Expert Syst., vol. 40, no. 5, Jun. 2023, Art. no. e13131.

[9] S. Baker and W. Xiang, ''Artificial intelligence of things for smarter healthcare: A survey of advancements, challenges, and opportunities,'' IEEE Commun. Surveys Tuts., vol. 25, no. 2, pp. 1261–1293, Mar. 2023.

[10] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, ''A comprehensive review of cyber-attacks and defensemechanisms for improving security in smart grid energy systems: Past, present and future,'' Electric Power Syst. Res., vol. 215, Feb. 2023, Art. no. 108975.

[11] D. K. Jain, S. Neelakandan, T. Veeramani, S. Bhatia, and F. H. Memon, ''Design of fuzzy logic based energy management and traffic predictive model for cyber physical systems,'' Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108135.

[12] M. Karatas, L. Eriskin, M. Deveci, D. Pamucar, and H. Garg, ''Big data for healthcare Industry 4.0: Applications, challenges and future perspectives,'' Expert Syst. Appl., vol. 200, Aug. 2022, Art. no. 116912.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

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

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

[13] M. Kumari, M. Singh, A. Grover, A. Sheetal, C. Goel, and Suvidhi, ‘‘The\ cyber physical systems and Industrial Internet of Things (IIoT),’’ in Securityand Resilience of Cyber Physical Systems. Boca Raton, FL, USA: CRCPress, 2022, pp. 1–12.

[14] E. U. Haque, M. S. Baig, A. Ahmed, A. Ahmad, M. Alajmi, Y. Y. Ghadi, H. K. Alkahtani, and A. Akhmediyarova, ‘‘Scalable EdgeIoT blockchain framework using EOSIO,’’ IEEE Access, vol. 12, pp. 41763–41772, 2024.

[15] A. A. Khalil, J. Franco, I. Parvez, S. Uluagac, H. Shahriar, and M. A. Rahman, ‘‘A literature review on blockchain-enabled security and operation of cyber-physical systems,’’ in Proc. IEEE 46th Annu. Comput, Softw., Appl. Conf. (COMPSAC), Jun. 2022, pp. 1774–1779.

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