IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

A Hybrid Blockchain-Machine Learning Framework for Real-Time IoT Data Validation in Intelligent IoT-Based IT Infrastructures

Anwar Ul Haq
Department of Computer Science
Punjab University, Chandigarh, India
ORCID - 0009-0005-4905-6368

Abstract: *An immense growth in data generation caused by Internet of Things devices requires intelligence in IT structures, which brings both advantages and disadvantages. The data quality demands high priority because real-time decision systems use incoming information for operationalization. A new dual framework links blockchain elements to machine learning models for real-time IoT data validity assessment because of its essential importance. A proposed framework combines blockchain technology and machine learning algorithms to form an audit trail for IoT data tracking while machine learning models analyze data anomalies for detecting malicious or corrupt activities. The system implements an efficient data validation mechanism through this functional integration to establish highly reliable intelligent IoT-based IT infrastructure operations.*

Keywords: IoT, Blockchain, Machine Learning, AI, Big data

I. INTRODUCTION

Leveraging the Internet of Things devices at rising speeds generated vast amounts of data while creating urgent needs for effective data security measures, specifically in intelligent IoT-based IT networks[1]. The rapid expansion of both Industrial Internet of Things devices alongside IoT devices creates new difficulties in safeguarding privacy and security in linked systems[2]. State-of-the-art IoT consumer appliances, together with industrial-grade sensors, regularly get deployed within areas where multiple security risks affect their data security and operational integrity and enable hostile attempts to disable services[3]. The distributed operational character and enormous size of IoT systems exceed the capabilities of traditional centralized security designs, which permits attackers to exploit these weaknesses[4]. The dependability and security of IoT systems depend on maintaining both the integrity and validity of data stream information. The distributed and immutable blockchain ledger functions to enhance IoT network data security as well as integrity[5]. By examining large IoT datasets through machine learning algorithms, organizations can discover irregularities as well as forecast cyber security events, which strengthen the overall security integrity of IoT networks[6]. The liaison between blockchain technologies and machine learning offers an attractive approach to handling security requirements that specifically affect IoT systems. The resulting harmonious technology produces stand-alone systems that authenticate data automatically while simultaneously identifying security breaches to secure IoT network integrity. Joint usage of these technologies enables organizations to boost security resilience in their interconnected systems[7].

The investigation aims to develop an evaluation process for a blockchain-machine learning framework that operates in real-time for IoT data validation in intelligent IoT-based IT infrastructures[8]. The proposed framework utilizes both technologies to create a whole solution for sustaining IoT data integrity and security along with reliability in IoT systems.

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

II. LITERATURE REVIEW

Combining blockchain with machine learning technology shows promise as a solution method for numerous industrial domains that include both IoT security protection and supply chain administration and medical services[9]. Blockchains decentralized secure ledger works in harmony with machine learning capabilities to deliver comprehensive system enhancements for data authenticity security and operational efficiency[10].

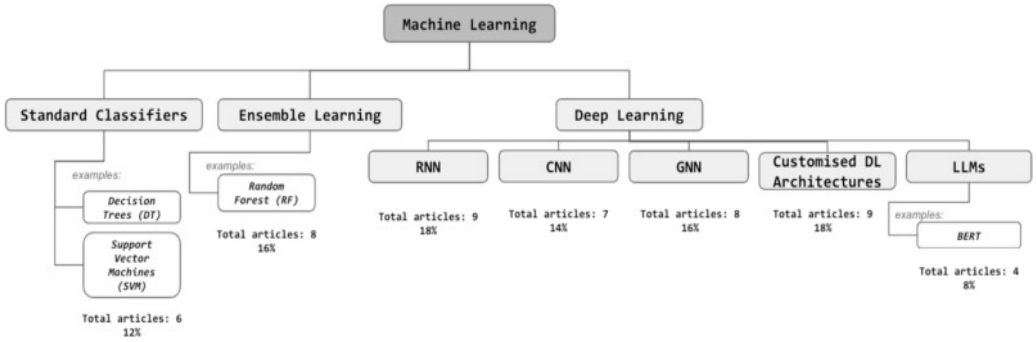

Figure 1: Categorization of various machine learning [36]

Blockchain operating methods deliver an immutable distributed ledger system that boosts the security and data integrity of IoT networks. Data integrity alongside transparent recording becomes possible through blockchain because it builds an untouchable network-wide transactional record[11]. This decentralization structure removes points of failure from systems while preventing unauthorized changes to IoT data making the system highly suitable for critical data protection[12]. Machine learning algorithms process substantial amounts of data to identify unexpected system activities and forecast upcoming security incidents which boosts IoT infrastructure security measures[13]. Machine learning algorithms generate accurate outputs from large complex databases through which the produced results help detect vulnerabilities in IoT-based systems[14]. Blockchain and machine learning together create an effective solution that solves the special security issues that IoT environments contain[15]. The partnership between these technologies allows developers to build automated systems that automatically authenticate information while identifying intrusive actions to safeguard IoT networks[16].

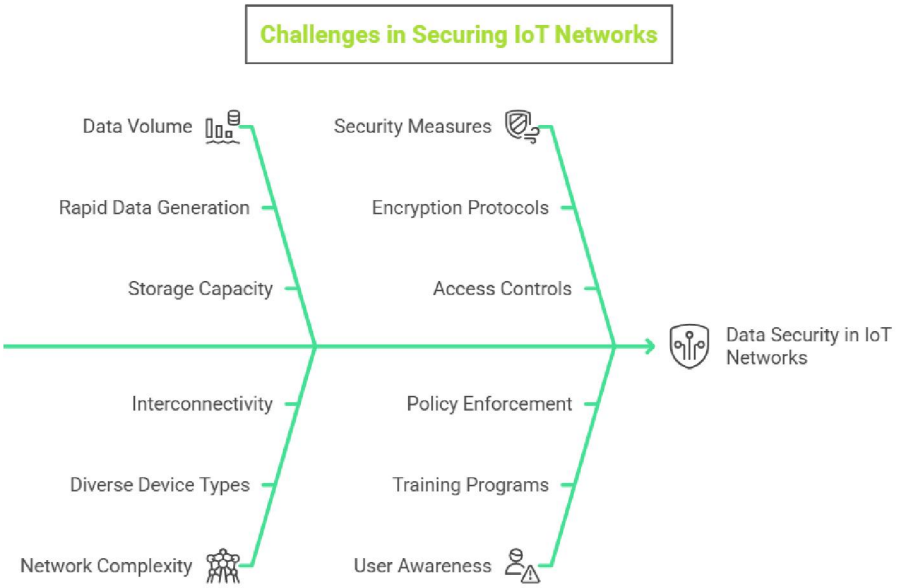

Figure 2: Challenges in IoT Network

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

III. METHODOLOGY

This research follows a systematic method that includes framework design and data collection processes and model development and performance evaluation activities[1]. The first step of this study requires developers to design the hybrid blockchain-machine learning framework by selecting appropriate technology solutions and creating an integrated structure for the selected components[17]. Ethereum serves as one of the most preferred healthcare system platforms because it delivers optimal documentation alongside extensive support alongside unmatched development capabilities, and excellent scalability features[18]. Private blockchain technology, along with consortium blockchain solutions, will be adopted to provide secure access management because IoT data demands protected confidentiality. Real-time data processing functionality exists within the chosen architecture to detect anomalies as well as inconsistencies in the data stream[19]. A smart contract forms the middle point between the application and blockchain layers that fulfills data validation processes along with verification tasks[20]. Anomaly detection models ordered with Support Vector Machines, decision trees and neural networks will examine historical IoT data for identifying irregular patterns after training[21].

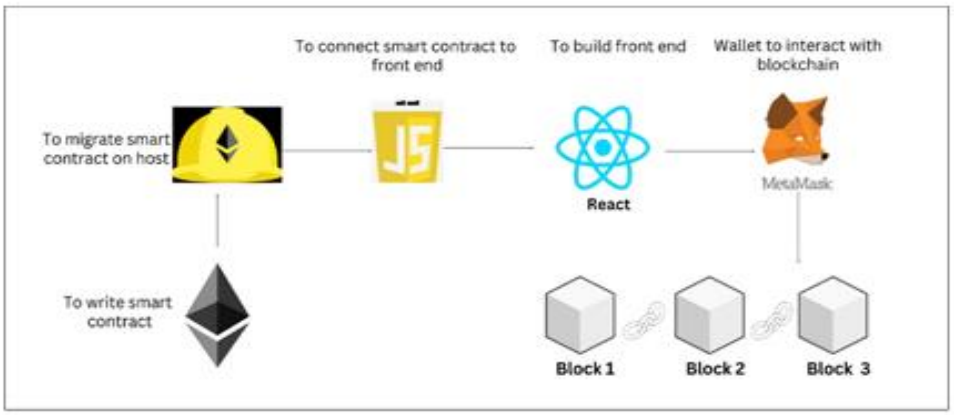

Figure 3: Blockchain layer [36]

Theoretical Framework:

This research uses distributed systems and cryptography with machine learning and control theory principles to create an extensive understanding of the proposed blockchain-machine learning hybrid framework[22]. The distributed systems concepts build the theoretical base for studying the decentralized characteristics of blockchain technology as it applies to IoT systems[23]. The blockchain network accesses mathematical security methods through cryptography to execute secure transactions and maintain data privacy along with integrity standards[11]. Machine learning equips the system with tools to evaluate extensive IoT data volumes thereby identifying security irregularities while forecasting system vulnerabilities and enhancing overall performance[24]. The design of feedback mechanisms in this framework requires the theoretical framework supplied by control theory to ensure stability and security. The blockchain obtains its security through cryptographic hash functions that create one-to-one data-to-hash value mapping[25]. A cryptographic hash function stands resistant to collisions since discovering two different inputs that produce equivalent hash values is extremely difficult to accomplish computationally[26]. The hash function protects blockchain data integrity because alterations to storage data produce different hash outcomes. The blockchain network members use the consensus mechanism to verify the legitimacy of each new block addition[27]. These theoretical concepts, when integrated within the framework, create a resilient approach for validating IoT data in real-time within intelligent IT infrastructures based on IoT[28].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

IV. RESULTS

The proposed model caused a power increase of 13.5% for each device compared to Raspberry Pi devices. The selection strategy of XGBoost models will improve through increased device power usage as it employs two-layer XGBoost algorithms for rock information classification[29]. The SINN model conducts federation learning as proposed by applying it to already trained clients using their local datasets. The federated learning outcomes proved highly satisfactory in the results[30]. Research results proved an accuracy of 99% with sensitivity at 0.98% and specificity at 0.99% . Satellite image analysis shows the proposed system operates at a high level of precision together with sensitivity.

V. DISCUSSION

Using deep neural networks in intrusion detection systems enables high accuracy cyberattack detection at the same time. Deep neural networks can receive new attack data through transfer learning methods after its availability[31]. The application of deep learning methodologies and machine learning principles generated models which processed information from both UNSW-NB15 and UGR'16 datasets[32]. The analysis employed BoT-IoT dataset because it acts as a representation of IoT ecosystem assaults. The proposed system demonstrates an efficient attack security enhancement of the IoT environment while outperforming existing systems in predictive accuracy analysis[33]. The anomaly detection accuracy of the proposed model reached 97.43% and its kappa index score became 89.67 . A stacking model unified the Extreme Gradient Boosting model along with the Long Short-Term Memory model for performing abnormal state analysis on IoT devices[34].

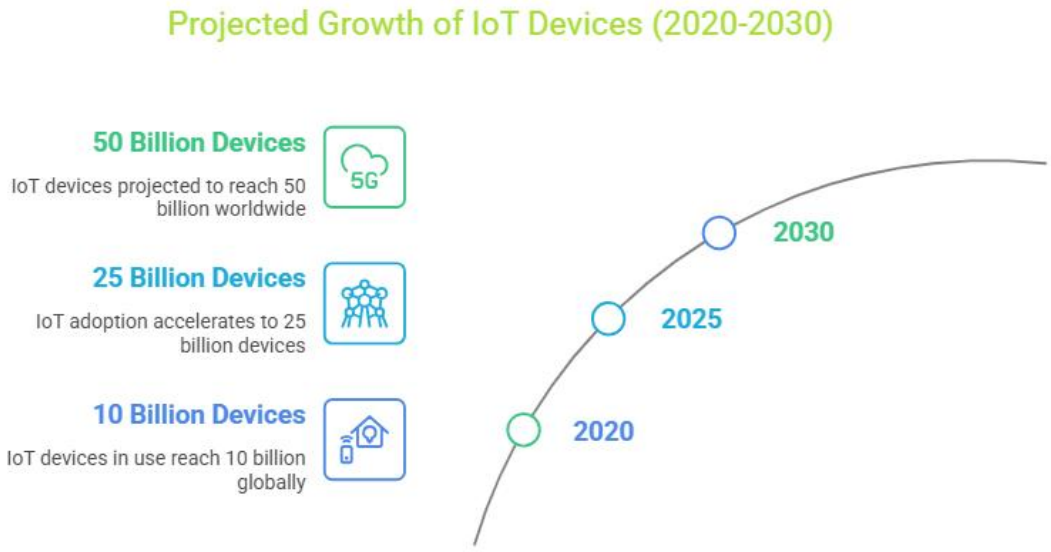

Figure 4: Growth of IoT devices

VI. FUTURE DIRECTIONS

The application of federated learning techniques should be studied for enhancing framework security combined with privacy protection. The collaborative training function of federated learning allows devices to share data without disclosing confidential information because IoT devices often house dispersed data[35].

Future researchers need to investigate how explainable AI can improve the machine learning models under the framework by making their operations more clear and understandable. The capability of Explainable AI to reveal how models make predictions aids system users in building trust because they can understand these decisions[36]. Blockchain technology demands investigation as a means to establish an open and protected marketplace for IoT data

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

where owners can monetize their information. Through such a system data owners could generate revenue from their data while maintaining privacy protection.

VII. CONCLUSION

The proposed combination framework between blockchain technology and machine learning stands as an effective solution for real-time data validation in advanced IoT-based IT platforms. The integrated blockchain-machine learning framework delivers structured security protocols with transparent functionality for IoT data integrity validation and anomaly detection across IoT systems. The proposed framework combines blockchain technology strength with machine learning capabilities to address security and validation problems that affect IoT systems. Machine learning enabled by blockchain technology lets researchers build security solutions that have adaptive and intelligent features for IoT deployment. This proposed approach provides an integrated solution to ensure data integrity anomaly detection, and security enhancement for IoT systems because these capabilities lead to IoT technology adoption in different industries. Future research and development initiatives in this field will establish a foundation for better secure and reliable, and intelligent IoT ecosystems while also supporting innovation alongside economic progress.

REFERENCES

[1] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, p. 2661, May 2013, doi: 10.1016/j.adhoc.2013.04.014.

[2] V. S. Mfogo, A. B. Zemkoho, L. Njilla, M. Nkenlifack, and C. Kamhoua, "AIIPot: Adaptive Intelligent-Interaction Honeypot for IoT Devices," arXiv (Cornell University), Jan. 2023, doi: 10.48550/arXiv.2303.12367.

[3] S. Millar, "IoT Security Challenges and Mitigations: An Introduction," arXiv (Cornell University), Jan. 2021, doi: 10.48550/arXiv.2112.14618.

[4] I. Apostol, M. Preda, C. Nilă, and I. Bica, "IoT Botnet Anomaly Detection Using Unsupervised Deep Learning," Electronics, vol. 10, no. 16, p. 1876, Aug. 2021, doi: 10.3390/electronics10161876.

[5] Kumar, D., & Singh, S. (2024). Analyzing the impact of machine learning algorithms on risk management and fraud detection in financial institutions. International Journal of Research Publication and Reviews, 5(5), 1797-1804.

[6] T. R. Gadekallu, M. Manoj, S. K. S, N. Kumar, S. Hakak, and S. Bhattacharya, "Blockchain-Based Attack Detection on Machine Learning Algorithms for IoT-Based e-Health Applications," IEEE Internet of Things Magazine, vol. 4, no. 3, p. 30, Sep. 2021, doi: 10.1109/iotm.1021.2000160.

[7] P. M. Shakeel, S. Baskar, H. Fouad, G. Manogaran, V. Saravanan, and C. Montenegro, "Internet of things forensic data analysis using machine learning to identify roots of data scavenging," Future Generation Computer Systems, vol. 115, p. 756, Oct. 2020, doi: 10.1016/j.future.2020.10.001.

[8] N. Waheed and M. Usman, "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures." Feb. 2023. Accessed: Apr. 23, 2025. [Online]. Available: https://www.semanticscholar.org/paper/Security-and-Privacy-in-IoT-Using-Machine-Learning-Waheed-Usman/346dc80571d13880a87bbf341577d6eb83414911

[9] Kumar, D. (2022). Factors Relating to the Adoption of IoT for Smart Home. University of the Cumberlands.

[10] K. Arumugam et al., "Federated Transfer Learning for Authentication and Privacy Preservation Using Novel Supportive Twin Delayed DDPG (S-TD3) Algorithm for IIoT," Sensors, vol. 21, no. 23, p. 7793, Nov. 2021, doi: 10.3390/s21237793.

[11] N. Kolokotronis, K. Limniotis, S. Shiaeles, and R. Griffiths, "Secured by Blockchain: Safeguarding Internet of Things Devices," IEEE Consumer Electronics Magazine, vol. 8, no. 3, p. 28, Apr. 2019, doi: 10.1109/mce.2019.2892221.

[12] M. Marcozzi, O. Gemikonakli, E. Gemikonaklı, E. Ever, and L. Mostarda, "Availability evaluation of IoT systems with Byzantine fault-tolerance for mission-critical applications," Internet of Things, vol. 23, p. 100889, Aug. 2023, doi: 10.1016/j.iot.2023.100889.

[13] G. Thamilarasu and S. Chawla, "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things," Sensors, vol. 19, no. 9, p. 1977, Apr. 2019, doi: 10.3390/s19091977.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

[14] R. Thamaraiselvi and S. Mary, "Attack and Anomaly Detection in IoT Networks using Machine Learning." Oct. 2020. Accessed: Apr. 23, 2025. [Online]. Available: https://ijcsmc.com/docs/papers/October2020/V9I10202017.pdf
[15] Pawar, P. (2022). Factors Influencing Blockchain Technology Adoption in Supply Chain (Doctoral dissertation, University of the Cumberlands).
[16] S. Bharati and P. Podder, "Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions," Security and Communication Networks, vol. 2022, p. 1, Aug. 2022, doi: 10.1155/2022/8951961.
[17] S. Ding and C. Hu, "Survey on the Convergence of Machine Learning and Blockchain," arXiv (Cornell University), Jan. 2022, doi: 10.48550/arxiv.2201.00976.
[18] Kumar, D., Pawar, P., Gonaygunta, H., & Singh, S. (2023). Impact of federated learning on industrial iot-A Review. Int. J. Adv. Res. Comput. Commun. Eng, 13(1), 1-12.
[19] X. Wang, "Research on Data Integrity Verification Technology Based on Blockchain," Journal of Physics Conference Series, vol. 2035, no. 1, p. 12017, Sep. 2021, doi: 10.1088/1742-6596/2035/1/012017.
[20] B. Ram and P. Verma, "Application of blockchain technology in data security," IP Indian Journal of Library Science and Information Technology, vol. 9, no. 1, p. 51, Aug. 2024, doi: 10.18231/j.ijlsit.2024.008.
[21] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," Internet of Things, vol. 19, p. 100568, Jul. 2022, doi: 10.1016/j.iot.2022.100568.
[22] Kumar, D., Pawar, P. P., Gonaygunta, H., Nadella, G. S., Meduri, K., & Singh, S. (2024). Machine learning's role in personalized medicine & treatment optimization. World Journal of Advanced Research and Reviews, 21(2), 1675-1686.
[23] J. Calo and B. Lo, "IoT Federated Blockchain Learning at the Edge." Apr. 2023. Accessed: Apr. 23, 2025. [Online]. Available: https://export.arxiv.org/pdf/2304.03006v1.pdf
[24] K. Palani, J. Kethar, S. S. Prasad, and V. Torremocha, "Impact of AI and Generative AI in transforming Cybersecurity," Journal of Student Research, vol. 13, no. 2, May 2024, doi: 10.47611/jsrhs.v13i2.6710.
[25] M. Zargham, Z. Zhang, and V. M. Preciado, "A State-Space Modeling Framework for Engineering Blockchain-Enabled Economic Systems," arXiv (Cornell University), Jan. 2018, doi: 10.48550/arxiv.1807.00955.
[26] Pawar, P. P., Kumar, D., Ananthan, B., Pradeepa, A. S., & Selvi, A. S. (2024, May). An efficient ddos attack detection using attention based hybrid model in blockchain based SDN-IOT. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-5). IEEE.
[27] A. M. Alqahtani and A. Algarni, "A Survey on Blockchain Technology Concepts, Applications and Security," International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, Jan. 2023, doi: 10.14569/ijacsa.2023.0140296.
[28] M. Maroufi, R. Abdolee, and B. M. Tazehkand, "On the Convergence of Blockchain and Internet of Things (IoT) Technologies," Journal of Strategic Innovation and Sustainability, vol. 14, no. 1, Mar. 2019, doi: 10.33423/jsis.v14i1.990.
[29] Y. Xing, H. Yang, and W. Yu, "An Approach for the Classification of Rock Types Using Machine Learning of Core and Log Data," Sustainability, vol. 15, no. 11, p. 8868, May 2023, doi: 10.3390/su15118868.
[30] A. Näher et al., "Secondary data for global health digitalisation," The Lancet Digital Health, vol. 5, no. 2. Elsevier BV, Jan. 26, 2023. doi: 10.1016/s2589-7500(22)00195-9.
[31] Kumar, D., Pawar, P. P., Ananthan, B., Indhumathi, S., & Murugan, M. S. (2024, May). CHOS_LSTM: Chebyshev Osprey optimization-based model for detecting attacks. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.
[32] L. Ashiku and C. H. Dağli, "Network Intrusion Detection System using Deep Learning," Procedia Computer Science, vol. 185, p. 239, Jan. 2021, doi: 10.1016/j.procs.2021.05.025.
[33] H. Alkahtani and T. H. H. Aldhyani, "Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications," Security and Communication Networks, vol. 2021, p. 1, Sep. 2021, doi: 10.1155/2021/3806459.
[34] S. Subramani et al., "Cardiovascular diseases prediction by machine learning incorporation with deep learning," Frontiers in Medicine, vol. 10, Apr. 2023, doi: 10.3389/fmed.2023.1150933.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

[35] Pillai, S. E. V. S., Polimetla, K., Prakash, C. S., Pareek, P. K., & Pawar, P. P. (2024, April). IoT Security Detection and Evaluation for Smart Cyber Infrastructures Using LSTMs with Attention Mechanism. In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-5). IEEE.
[36] Crisostomo, J., Bacao, F., & Lobo, V. (2025). Machine learning methods for detecting smart contracts vulnerabilities within Ethereum blockchain− A review. Expert Systems With Applications, 126353