iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 12 **Issue:** V **Month of publication:** May 2024

**DOI:** https://doi.org/10.22214/ijraset.2024.62601

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 12 Issue V May 2024- Available at www.ijraset.com*

# Malicious Node Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs

Akash Pawar[1], Onkar Ladkat[2], Shendage Prashant[4], Tejas Jadhav[5], Prof. Suryavanshi A.P.[6]
*Department of Computer Engineering, HSBPVT'S GOI FOE, SPPU, Maharashtra, India*

***Abstract:*** ***Wireless Sensor Networks (WSNs) present unique opportunities for a broad spectrum of applications such as industrial automation, situation awareness, tactical surveillance for military applications, environmental monitoring, chemical or biological detection etc., Wireless Sensor Networks (WSNs) consist of hundreds of tiny nodes having the capability of sensing, computation and wireless communications. Deployed in a hostile environment, individual nodes of a wireless sensor network (WSN) could be easily compromised by the adversary due to the constraints such as limited battery lifetime, memory space and computing capability. It is critical to detect and isolate the compromised nodes in order to avoid being misled by the falsified information injected by the adversary through compromised nodes. However, it is challenging to secure the flat topology networks efficiently because of the poor scalability and high communication overhead. Since security and performance issues are a big concern in the case of wireless sensor networks, emphasis has been given to the scheme based on Weighted-Trust Evaluation (WTE). Extensive simulation is performed using MATLAB, to verify performance and efficiency of WTE by varying various parameters***

***Keywords: Malicious Node Detection, Machine Learning, Wireless Sensor Networks (WSNs),Blockchain Technology, Data Integrity, Data Security, Trustworthiness, Sensor Node Security, Network Security, Secure Data Retrieval.***

## I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of very small devices, called sensor nodes, that are battery powered and are equipped with integrated sensors, a data processing unit, a small storage memory, and short-range radio communication. Typically, these sensors are randomly deployed in the field. They form an unattended wireless network, collect data from the field, partially aggregate them, and send them to a sink that is responsible for data fusion. It is critical to detect and isolate the compromised nodes in order to avoid being misled by the falsified information injected by the adversary through compromised nodes. Sensor networks have applications in emergencyresponse networks, energy management, medical monitoring, logistics and inventory management, and battlefield management. In contrast to traditional wireless networks, special security and performance issues have to be carefully considered for sensor networks. For example, due to the unattended nature of sensor networks, an attacker could launch various attacks and even compromise sensor devices without being detected. Therefore, a sensor network should be robust against attacks, and if an attack succeeds, its impact should be minimized. In other words, compromising a single sensor node or few sensor nodes should not crash the entire network. Another concern is about energy efficiency. In a WSN, each sensor node may need to support multiple communication models including unicast, multicast, and broadcast. Therefore, due to the limited battery lifetime, security mechanisms for sensor networks must be energy efficient. Especially the number of message transmissions and the amount of expensive computation should be as few as possible. In fact, there are a numbers of attacks an attacker can launch against a wireless sensor network once a certain number of sensor nodes have been compromised [4]. In literature, Vol-9 Issue-6 2023 IJARIIE-ISSN(O)2395-4396 21947 www.ijariie.com 221 for instance, HELLO flooding attacks, sink hole attacks, Sybil attack, black hole attack, wormhole attacks, or DDoS attacks are options for an attacker. These attacks lead to anomalies in network behaviors that are detectable in general.

## II. LITERATURE SURVEY

1.Ganeriwal et al. proposed a reputation-based framework for data integrity in WSNs. The proposed reputation system takes information collected by each node using a Watchdog mechanism (for direct monitoring and observations) to detect invalid data and uncooperative nodes.

©IJRASET: All Rights are Reserved 

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 12 Issue V May 2024- Available at www.ijraset.com*

2.Yao et al. proposed a parameterized and localized trust management scheme for WSN security, particularly for secure routing, where each node only maintains highly abstracted parameters to evaluate its neighbours. 3.Aivaloglou and Grizzlies proposed a hybrid trust and reputation management protocol for WSNs by combining certificate-based and behaviour-based trust evaluations. However, [1-3] cited above only considered a node's QoS property in trust evaluation. Also, the analysis was conducted based on a flat WSN architecture which is not scalable. 4&5Liu et al. [4] and Moraru et al. proposed trust management protocols and applied them to geographic routing in WSNs. However, no hierarchical trust management was considered for managing clustered WSNs. Their work again evaluated trust based on QoS aspects only such as packet dropping and the degree of cooperativeness, while our work considers both QoS and social trust for trust evaluation of a SN. 6. Capra et al. discussed the notion of human trust which could be formed from three sources: direct experiences, credentials, and recommendations. In particular recommendations are trusting information coming from other nodes in the social context. We consider only two sources in our notion of trust, namely, direct experiences and recommendations since it is hard for SNs with limited resources to carry credentials. A significant difference of Capra's work from our work is that we specifically consider individual QoS and social trust property, say, X, and devise specific trust aggregation protocols using direct experiences and recommendations to form trust property X, while Page 22 Capra used the three sources of information to form human trust. Moreover, because different trust properties have their own intrinsic trust nature and react differently to trust decay over time, we identify the best way for each trust property X to take in direct experiences and recommendations information so that the assessment of trust property X would be the most accurate against actual status in trust property X. Another significant difference is that we consider trust formation as the issue of forming the overall "trust" out of individual social and QoS trust properties, while Capra considered it as the issue of forming human trust out of the three sources of trust information. 7.H. Hu et al. proposed weighted trust approach here each SN has a weight associated with it representing the trustworthiness of its sensor reading output. The system periodically calculates the average sensor reading output by taking a weighted summation out of all sensor reading outputs. The weight associated with a SN is dynamically updated according to the deviation of the SN's output from the average output. A larger deviation results in a lower weight. Once the weight of a SN falls below a threshold, the SN is considered a malicious node. The main drawback of this approach is a high false positive probability may result.

## III. PROBLEM STATEMENT

Just as the wireless sensor networks provide a large number of advantages it also comes with few drawbacks. One among them is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. In the network if few nodes get compromised the whole network can be toppled unless the compromised nodes are removed from the network soon. In order to do so the compromised nodes should be identified using suitable algorithm and be removed. Sometimes the normal nodes might send the wrong data in case of temporary interruption in communication channel. Suitable algorithm should be used to ensure the proper detection of malicious nodes and avoid misdetection.

## IV. EXISTING MODEL

*1)* Machine Learning-based Malicious Node Detection: This involves using machine learning algorithms to analyse data collected by sensor nodes and identify those behaving abnormally or sending false information. This can help isolate and remove malicious nodes from the network before they can disrupt operations.

*2)* Distributed Data Storage Using Blockchain: Blockchain technology is employed to create a secure and tamper-proof ledger for storing sensor data. This ensures data integrity and prevents unauthorized modification by malicious actors.

## V. WSN MODEL

*1)* Sensor Node: A sensor node is a node in a wireless sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network.

*2)* Cluster Head: Sensor nodes are portioned into clusters and a cluster head is elected using a distributed algorithm. All nodes in the communication range of the cluster head belong to its cluster. Cluster head acts as interface between sensor nodes and base station.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 12 Issue V May 2024- Available at www.ijraset.com*

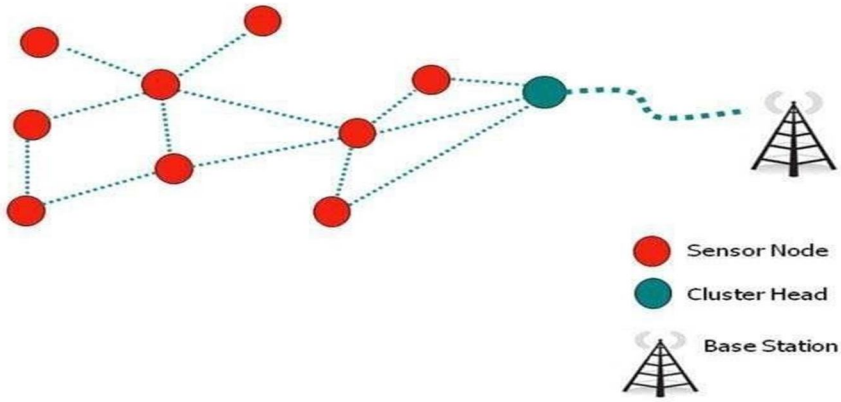



Fig 1. WSN Model

## VI. PROPOSED SYSTEM

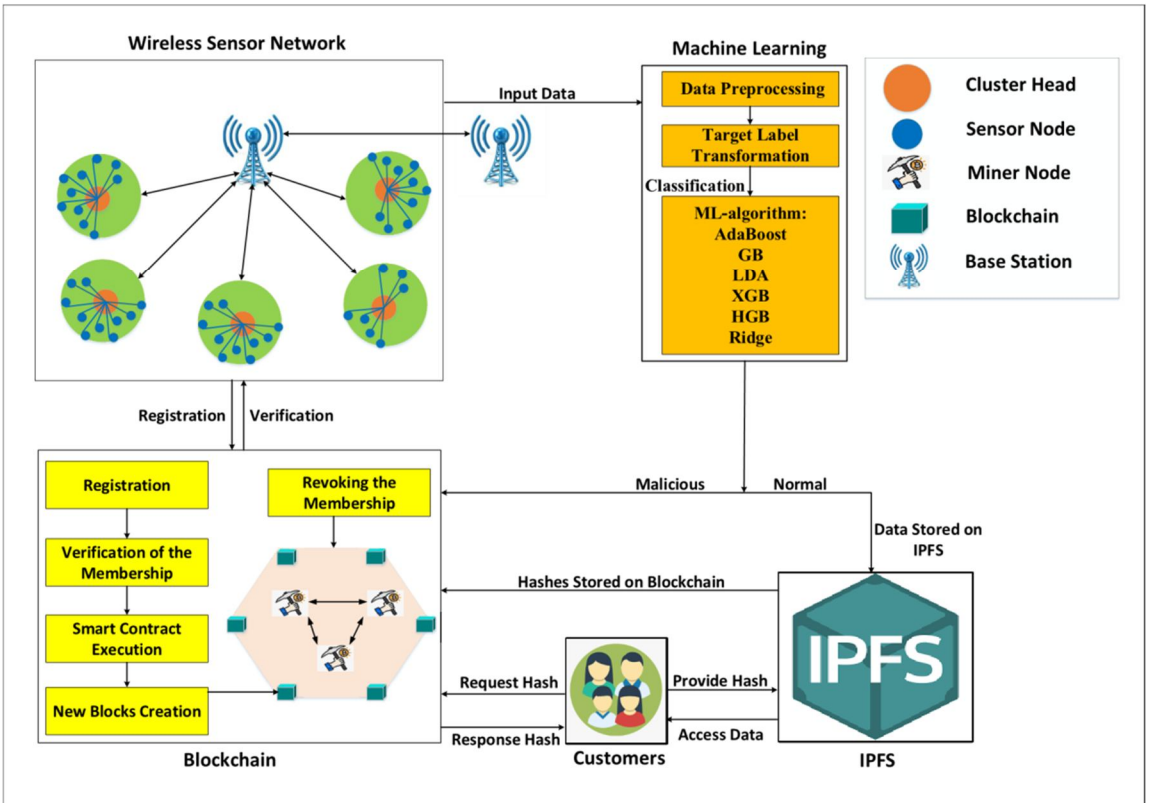



Fig : . PROPOSED MODEL

## VII. SOFTWARE REQUIREMENTS

1. Programming Languages
2. Machine Learning Libraries
3. Blockchain Development Tools
4. Distributed Data Storage
5. Development Environments
6. Version Control
7. Database
8. Networking
9. Security
10. Documentation and Reporting

©IJRASET: All Rights are Reserved 

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 12 Issue V May 2024- Available at www.ijraset.com*

## VIII. BLOCK DIAGRAM

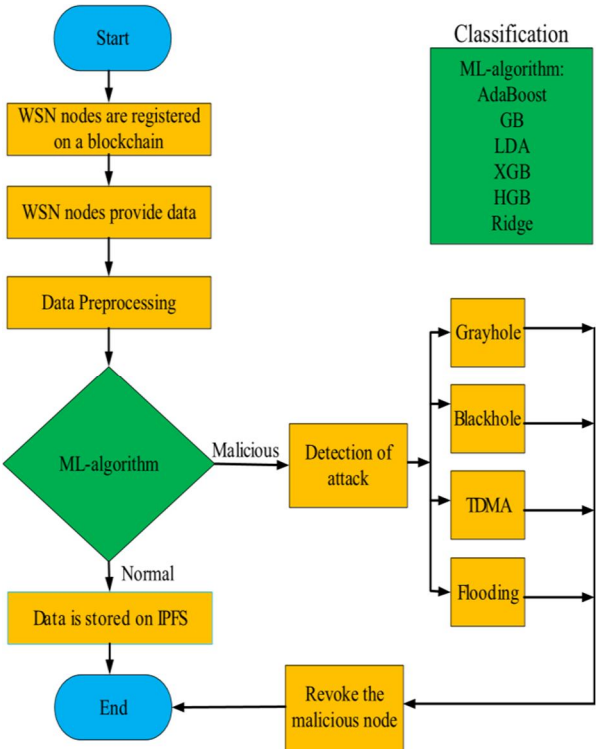



Fig . Block Diagram

## IX. FINAL RESULTS

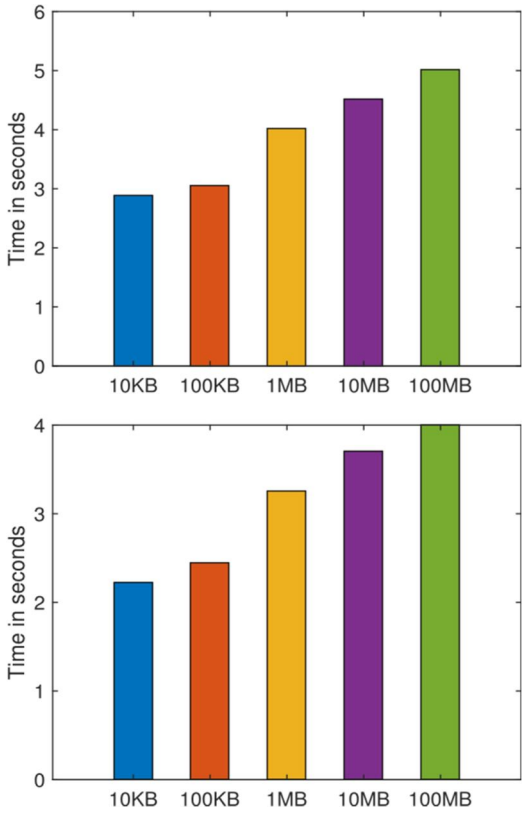



Fig: Comparison of time consumed in uploading files on IPFS

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

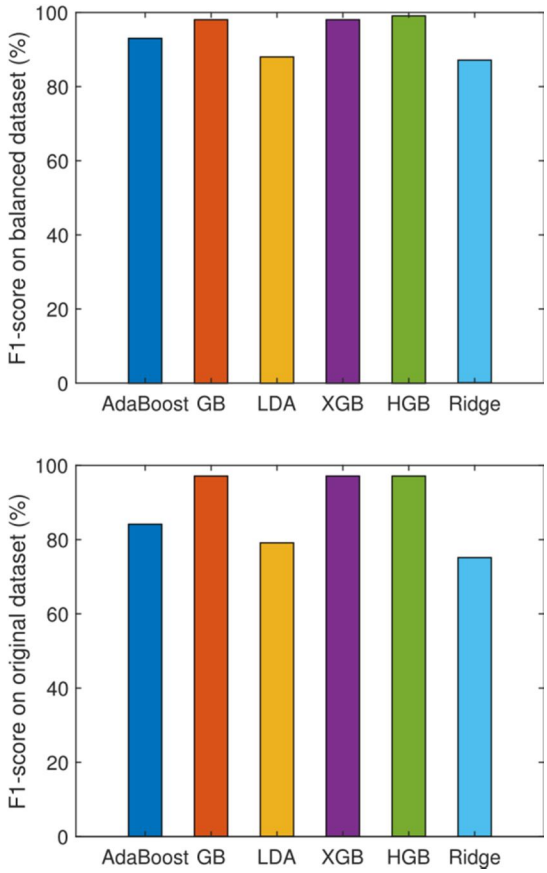
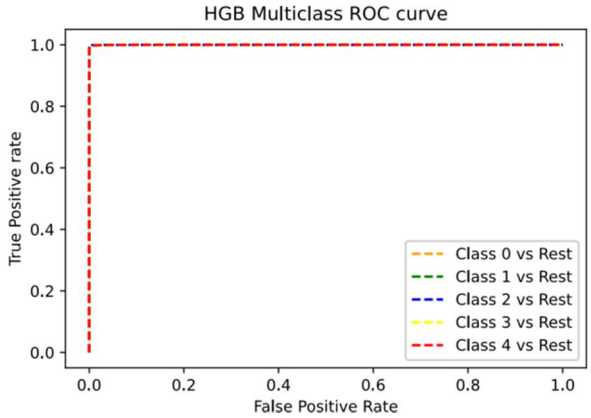



Fig: F1-score of classifiers on the balanced dataset. (b) F1-score of classifiers on the original dataset

## X. EFFORT ESTIMATE TABLE




## XI. CONCLUSION

This study proposes a network model to detect malicious nodes in WSNs. SNs and CHs are registered on BSs that are responsible for monitoring the whole network and storing the credentials of the network nodes. In addition to this, blockchain technology is deployed on BSs. Both the verification and registration of nodes are done through blockchain. Moreover, a consensus mechanism, VBFT, is used to validate the transactions, which reduces transaction costs. Moreover, the network nodes' credentials and the hash values that IPFS produces are stored in the blockchain. Furthermore, the ML classifier, referred to as HGB, is utilized to identify malicious nodes. The simulation results show that the HGB classifier outperforms AdaBoost, GB, LDA, XGB, and ridge classifiers in terms of accuracy, precision, recall, micro-F1 score, and macro-F1 score.

©IJRASET: All Rights are Reserved 

In the proposed work, individual classifiers are used for classification, which does not provide enhanced efficiency. Moreover, the proposed work lacks in providing the vulnerability analysis of the smart contracts, which deteriorates the practicality of the work in the real world. Moreover, the monitoring of the WSN/IoT systems is beyond our scope at the current instant. In the future, to tackle the mentioned issues, a stacking model will be used in WSNs for performing more efficient malicious node detection. Furthermore, the Oyente tool will be used to assess the smart contracts' vulnerabilities. Moreover, this research will be conducted in various sectors using real-world networks. Besides, we aim to perform WSN/IoT system monitoring, as in [68], in the future.

## XII. FUTURE SCOPE

Deep Learning: Utilize deep learning algorithms like Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) to analyze complex sensor data and identify subtle anomalies that might indicate malicious behavior.

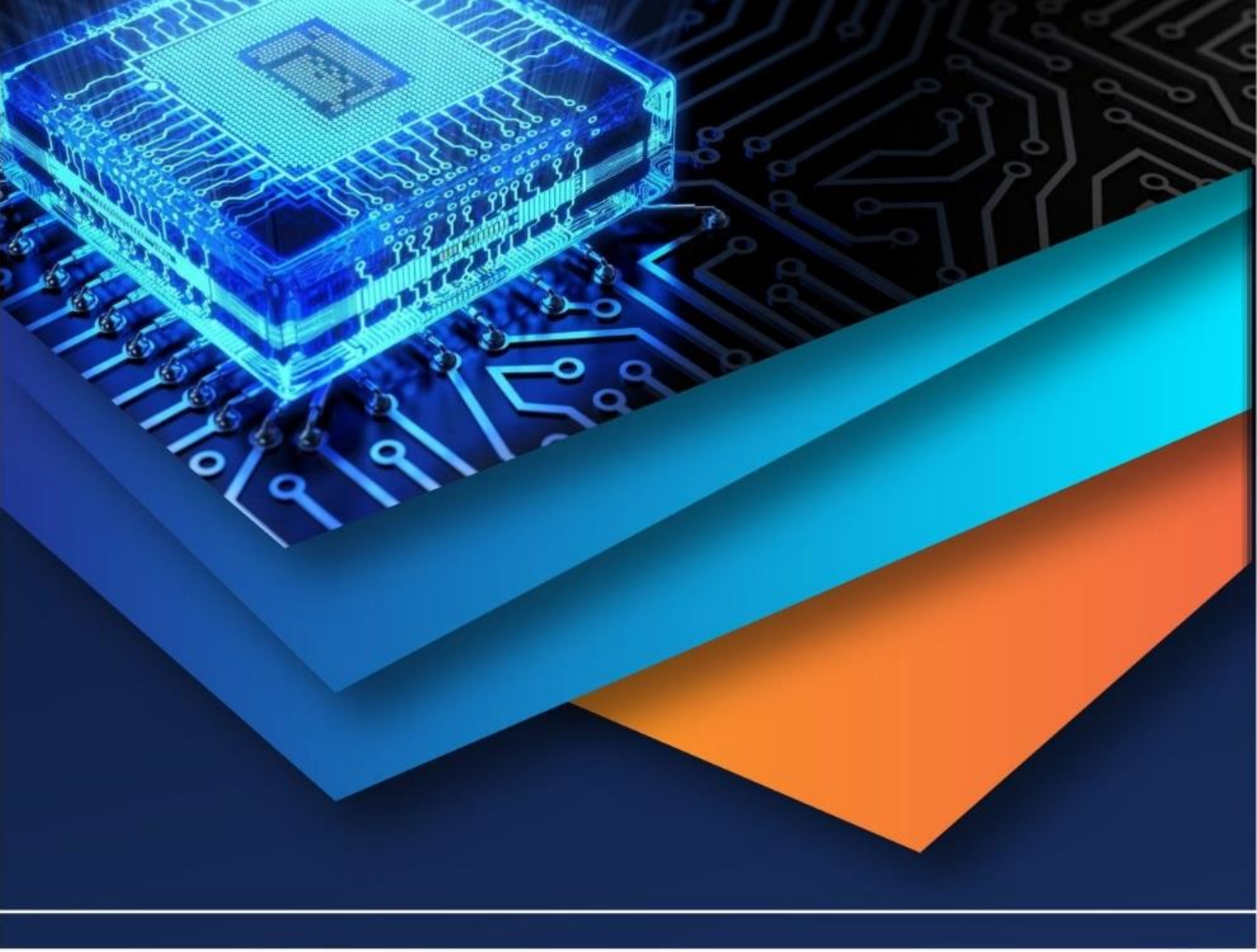
Federated Learning: Implement federated learning where local models are trained on individual sensor nodes and only the model updates are shared with a central server. This can improve privacy and reduce communication overhead.

Unsupervised Anomaly Detection: Explore unsupervised anomaly detection techniques that can identify malicious nodes without the need for labeled training data, which can be scarce in WSNs.

## REFERENCES

[1] O. J. Pandey, V. Gautam, S. Jha, M. K. Shukla, and R. M. Hegde, ‘‘Time synchronized node localization using optimal H-node allocation in a small world WSN,’’ IEEE Commun. Lett., vol. 24, no. 11, pp. 2579–2583, Nov. 2020, doi: 10.1109/LCOMM.2020.3008086.
[2] L. Xiong, N. Xiong, C. Wang, X. Yu, and M. Shuai, ‘‘An efficient lightweight authentication scheme with adaptive resilience of asynchronization attacks for wireless sensor networks,’’ IEEE Trans. Syst., Man, Cybern., Syst., vol. 51, no. 9, pp. 5626–5638, Sep. 2021, doi: 10.1109/TSMC.2019.2957175.
[3] H. Wang, P. Tu, P. Wang, and J. Yang, ‘‘A redundant and energyefficient clusterhead selection protocol for wireless sensor network,’’ in Proc. 2nd Int. Conf. Commun. Softw. Netw., 2010, pp. 554–558, doi: 10.1109/ICCSN.2010.46.
[4] S. A. Sert, E. Onur, and A. Yazici, ‘‘Security attacks and countermeasures in surveillance wireless sensor networks,’’ in Proc. 9th Int. Conf. Appl. Inf. Commun. Technol. (AICT), Oct. 2015, pp. 201–205.
[5] S. A. Sert, C. Fung, R. George, and A. Yazici, ‘‘An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks,’’ in Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE), Jul. 2017, pp. 1–6.
[6] R. Alkhudary, ‘‘Blockchain technology between Nakamoto and supply chain management: Insights from academia and practice,’’ SSRN Electron. J., pp. 1–12, Jul. 2020, doi: 10.2139/ssrn.3660342.
[7] Z. Abubaker, N. Javaid, A. Almogren, M. Akbar, M. Zuair, and
[8] J. Ben-Othman, ‘‘Blockchained service provisioning and malicious node detection via federated learning in scalable internet of sensor things networks,’’ Comput. Netw., vol. 204, Feb. 2022, Art. no. 108691.
[9] A. S. Yahaya, N. Javaid, M. U. Javed, A. Almogren, and A. Radwan, ‘‘Blockchain based secure energy trading with mutual verifiable fairness in a smart community,’’ IEEE Trans. Ind. Informat., vol. 18, no. 11, pp. 7412–7422, Nov. 2022.
[10] Z. Abubaker, A. U. Khan, A. Almogren, S. Abbas, A. Javaid, A. Radwan, and N. Javaid, ‘‘Trustful data trading through monetizing IoT data using BlockChain based review system,’’ Concurrency Comput., Pract. Exper., vol. 34, no. 5, p. e6739, Feb. 2022.
[11] S. Abbas, N. Javaid, A. Almogren, S. M. Gulfam, A. Ahmed, and A. Radwan, ‘‘Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things,’’ IEEE Access, vol. 9, pp. 139739–139754, 2021.
[12] Z. Li, A. V. Barenji, and G. Q. Huang, ‘‘Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform,’’ Robot. Comput.-Integr. Manuf., vol. 54, pp. 133–144, Dec. 2018.
[13] A. Welligton dos Santos Abreu, E. F. Coutinho, and C. Ilane Moreira Bezerra, ‘‘Performance evaluation of data transactions in blockchain,’’ IEEE Latin Amer. Trans., vol. 20, no. 3, pp. 409–416, Mar. 2022, doi: 10.1109/TLA.2022.9667139.
[14] G. Kumar, R. Saha, M. Rai, R. Thomas, and T. H. Kim, ‘‘Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics,’’ IEEE Internet Things J., vol. 6, no. 4, pp. 6835–6842, Aug. 2019, doi:
[15] 10.1109/JIOT.2019.2911969.
[16] J. Benet, ‘‘IPFS–content addressed, versioned, P2P file system,’’ 2014, arXiv:1407.3561.
[17] G. Kolumban-Antal, V. Lasak, R. Bogdan, and B. Groza, ‘‘A secure and portable multi-sensor module for distributed air pollution monitoring,’’ Sensors, vol. 20, no. 2, p. 403, Jan. 2020, doi: 10.3390/s20020403.
[18] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, and Y. Zhang, ‘‘A blockchainbased nonrepudiation network computing service scheme for industrial IoT,’’ IEEE Trans. Ind. Informat., vol. 15, no. 6, pp. 3632–3641, Jun. 2019, doi: 10.1109/TII.2019.2897133.
[19] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, ‘‘A blockchain-based location privacy protection incentive mechanism in crowd sensing networks,’’ Sensors, vol. 18, no. 11, p. 3894, 2018, doi: 10.3390/s18113894.
[20] D. P. Kumar, A. Tarachand, and C. S. R. Annavarapu, ‘‘Machine learning algorithms for wireless sensor networks: A survey,’’ Inf. Fusion, vol. 49, pp. 1–25, Sep. 2019.
[21] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, ‘‘On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance,’’ Comput. Netw., vol. 191, May 2021, Art. no. 108005.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)