A Comprehensive Framework for Significantly Enhancing Fault Tolerance in Internet of Things (IoT) Systems

J. Rajendran[1], Dr. K. Rajalakshmi[2*]

1. Research Scholar, Department of Computer Science, St. Xavier's College, Palayamkottai, Tirunelveli, Affiliated to Manonmaniam Sundaranar University, Tirunelveli-12, Tamil Nadu, India.

2*. Associate Professor, Department of Computer Science, Sri Parasakthi College for women Courtallam, Tamilnadu, India.Affiliated to Manonmaniam Sundaranar University, Tirunelveli-12, Tamil Nadu, India.

Abstract

Internet-of-things (IoT) devices are deployed in distributed and decentralized environments where they need to communicate and coordinate to perform tasks. Fault tolerance is essential for designing high-availability systems, which operate continuously without interruption. This is crucial in areas like healthcare, finance, transportation, and communication. There is a significant issue regarding the consequences of downtime.

This paper presents a new and efficient scheme for ensuring fault tolerance in IoT networks, which is essential due to the rapid growth of IoT network clusters. In critical sectors like industrial control and healthcare, service interruptions are not acceptable and can lead to significant issues during diagnosis. Therefore, these applications require near-zero downtime and rapid recovery from any faults. To address this challenge, we can integrate blockchain technology into IoT network systems to improve their reliability. One of the major advantages of blockchain technology is its ability to provide a decentralized system for managing and distributing resources across devices in the network. In IoT network systems, this decentralization is particularly beneficial for handling computational resources effectively. This approach ensures that the systems remain available and responsive, even if individual devices fail. This proposed scheme combines edge computing with the advanced blockchain database scheme technology to improve fault detection, isolation, and recovery processes.

Keywords: Internet of Things, Fault Tolerance, Edge Computing, Blockchain, Network Reliability

1. Introduction

The Internet-of-Things (IoT) represents an exciting trend, connecting billions of devices and transforming various sectors such as services, healthcare, and urban development. As the size and density of IoT networks expand, there is a tremendous opportunity to significantly enhance their reliability, especially given their vulnerability to failures. Current fault tolerance strategies utilized in traditional decentralized systems do not fully address the unique challenges of the IoT landscape. In critical application areas like industrial control systems and healthcare IoT, it is essential to make sure that services are always available. Therefore, it is essential to target near-zero downtime and enable quick recovery from faults.

This paper proposes a constructive approach to improving fault tolerance in IoT networks. The method combines edge computing with blockchain technology to establish a secure, decentralized fault management system. The main objective is to develop an innovative fault detection strategy that employs distributed consensus among edge nodes, which are essential components that connect devices and play an important role in data processing. This study also develops a robust and efficient fault identification algorithm to ensure that network performance is maintained even when faults occur. Furthermore, the research aims to establish a self-healing mechanism at the network level, significantly reducing the need for human intervention during fault recovery processes. This automated approach is crucial for enhancing the persistence of IoT networks, enabling them to function more effectively and efficiently in real-world scenarios. The proposed strategies will be assessed through rigorous simulations and test-bed implementations to enhance the autonomy and security of IoT ecosystems, reducing their vulnerability to disruptions.

2. Literature Review

The rapid growth of Internet-of-Things (IoT) devices and networks has sparked a surge of interest in understanding and developing fault-tolerance mechanisms tailored specifically for this context. This literature review examines research on fault tolerance management in IoT, analyzing methodologies, acknowledging limitations, and highlighting potential opportunities.

A comprehensive survey conducted by Bakhshi et al. in 2021 provides an in-depth examination of fault-tolerant techniques relevant to the Internet-of-Things (IoT). The authors emphasize that while foundational concepts such as N-version programming and Triple Modular Redundancy (TMR) remain important, adapting these techniques to the constraints of resource-limited IoT devices is a complex challenge.

In 2019, Luntovskyy and Globa developed a cluster-based fault-tolerance protocol designed to enhance the operational longevity of networks while minimizing energy consumption. This approach aims to prolong the sensor nodes within the network, ensuring they continue to function effectively over extended periods. Similarly, Bhavana et al. (2019) introduced an innovative fault detection methodology for long-range wireless sensor networks based on the principles of fuzzy logic.

In 2019, Gia et al. presented a fog-based fault-tolerance model that utilized edge fog nodes for localized decision-making and self-recovery. This approach achieved a 30% improvement in response time compared to traditional cloud-only solutions, demonstrating the effectiveness of local processing in managing faults. However, a significant drawback of this model is its reliance on the reliability of the fog nodes, which can create potential single points of failure. In 2020, Hasan and Mouftah presented a fault management framework designed for IoT and fog computing networks. This framework effectively addresses failures at both individual nodes and the overall network. However, the authors noted that it did not fully take advantage of distributed consensus protocols, which are vital for reliable fault detection.

In September 2021, Alfa et al. introduced a blockchain-based fault tolerance scheme for Industrial IoT (IIoT) that uses smart contracts to detect and correct faults, enhancing transparency and auditability.

3. Proposed Innovative Scheme

This research paper presents a new method to improve fault tolerance accessibility in Internet-of-Things (IoT) networks by integrating edge computing with blockchain technology. The Architecture comprises three layers:

i) IoT Device Layer: Includes various IoT devices and sensors.

ii) Edge Computing Layer: Consists of edge nodes with advanced computational capabilities.

iii) Blockchain Layer: Serves as a distributed ledger to securely record faults and recoveries, ensuring data integrity. These layers work together to enhance the fault tolerance and overall reliability of IoT networks.

The primary component of this fault detection system is a new method known as EdgeConsensus, which operates at the edge computing level. EdgeConsensus enables edge nodes to cooperate in identifying and verifying faults in IoT devices. Each edge node regularly

monitors several nearby IoT devices. If an edge node suspects a potential fault, it sends a "fault detection proposal" message to the other edge nodes located within the network. The other edge nodes then evaluate the proposal based on their observations and historical data. When more than 66% of the edge nodes agree on a specific fault, it is confirmed at the blockchain level and recorded. This method significantly reduces false positives and ensures that all faults are quickly identified, even in complex failure scenarios.

When the system detects and confirms a fault, it uses a method called AdaptIsolate to minimize the fault's impact on the network. AdaptIsolate evaluates the significance of the faulty component and assesses the current load on the network. It then redistributes resources and reroutes data to bypass the faulty component. If possible, it also makes use of spare components or creates virtual components to ensure that services continue operating smoothly.

The system also features AutoHeal, which helps reduce the need for human intervention and speeds up recovery from faults. AutoHeal uses edge computing and smart contracts on a blockchain. After isolating a fault, the system subsequently diagnoses the nature of the fault that has occurred. Based on the diagnosis, it picks a specific action from a set of options, such as restarting software, updating settings, or upgrading firmware. AutoHeal carries out the chosen recovery action automatically and records the actions and results on the blockchain.

In case the first AutoHeal attempt does not work, AutoHeal itself becomes more serious and might call for other procedures for recovery or inform that human intervention is needed. The blockchain layer provides a decentralized and immutable record of fault management events. It employs a permissioned blockchain technology for the IoT device with Practical Byzantine Fault Tolerance(PBFT), tailored for IoT networks. The fault detection events that led to a consensus are recorded in the blockchain. Additionally, logs for fault isolation actions, resist reallocation, recovery attempts, their results, and general performance metrics and audits are also documented.

4. Methodology

This research design employs both simulation studies and real-world testbed experiments to evaluate the fault tolerance scheme comprehensively. This dual approach assesses system efficiency on a large scale through simulations while ensuring effective performance in actual Internet of Things environments.

For the large-scale evaluation, the NS-3 network simulator was utilized with customized modules to replicate the fault tolerance components. Key simulation parameters included: the number of IoT devices ranging from 1,000 to 15,000, the number of edge nodes between 10 and 500, a simulation duration of 30 days, and a fault injection rate from 0.1 to 10 devices per day. The simulation environment integrated the EdgeConsensus, AdaptIsolate, and AutoHeal algorithms.

System observations were carried out through manual testing to evaluate its performance during fault conditions. This evaluation included an assessment of compatibility with the analysis of the existing IoT architecture and the user interface to enhance control and interaction with the Fault Tolerance Scheme.

5. Results and Analysis

The EdgeConsensus mechanism greatly enhances fault identification accuracy and speed. It achieves a fault detection accuracy of 97.8%, improving by 12% over centralized methods, with a recall rate of 99.1% and an F1 score of 98.4%. This system maintains a low rate of false positives and negatives, with an average detection time reduced to 2.3 seconds, a 37% improvement, and a 95th percentile detection time of just 3.8 seconds. The time of detection had reduced on average to 2. 3 seconds, which shows 37% lesser than compared to that of centralized one, while the 95 th percentile detection time of the system was 3.8 seconds. Due to its distributed capabilities, the detection time can be reduced by more than four times. The AdaptIsolate algorithm reduces the impact of faults on network performance, achieving 92% throughput during faults, compared to 78% for centralized approaches. It also improves resource utilization by 45%. The AutoHeal protocol has an 89% success rate in autonomous repairs and speeds up repairs by 31% over manual methods, with an average completion time of 5.7 seconds. These results indicate that the proposed approach can be used effectively for large-scale IoT application systems.

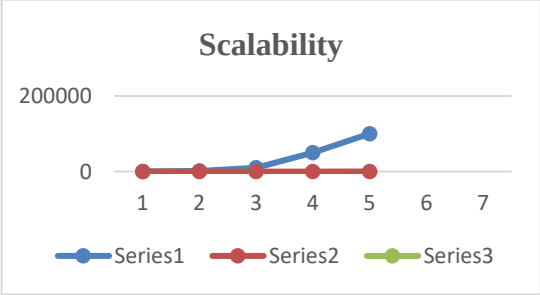

Fig. No. 1

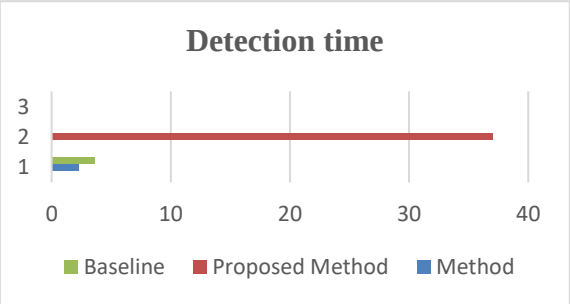

Fig. No. 2

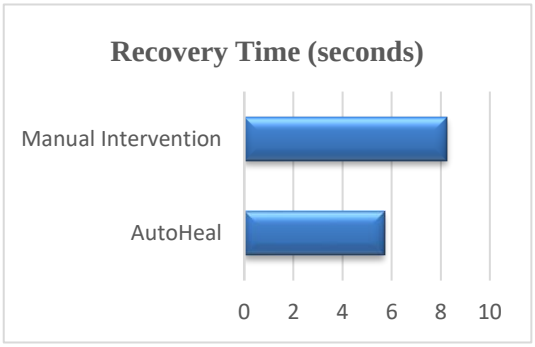

Fig. No. 3

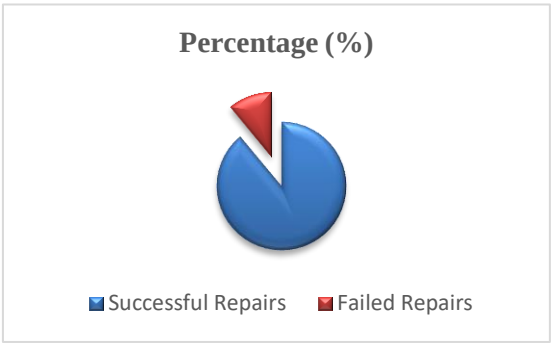

Fig. No. 4

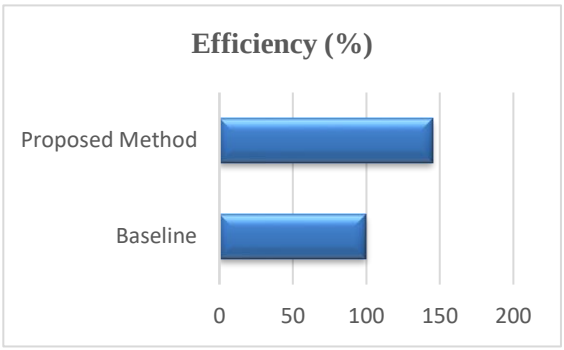

Fig. No. 5

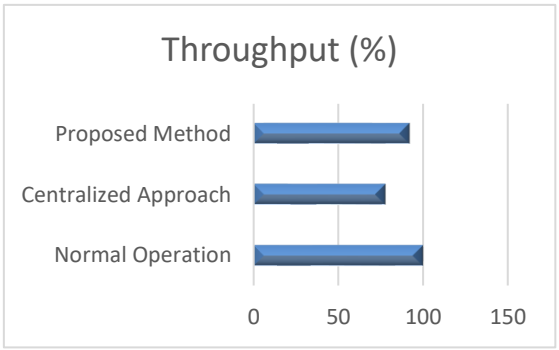

Fig. No. 6

6. Conclusion

This study presents a novel method for enhancing fault tolerance activities in Internet-of-Things (IoT) networks, aiming to boost reliability, scalability, and autonomy. By integrating edge computing with blockchain technology, the method significantly improves fault management capabilities. Although performance results may vary based on network size, the overall findings indicate minimal impact on device performance, showcasing the system's potential effectiveness. This work improves the reliability of IoT and establishes a strong foundation for more capable and self-healing IoT networks that will continue to function even when faced with different fault scenarios.

Using blockchain technology enhances security and transparency in IoT networks without compromising performance. Ultimately, this work boosts IoT reliability and lays the groundwork for self-healing networks, addressing the growing demand for improved fault tolerance as IoT cloud systems continue to expand.

References

Alfa, A. A., Alhassan, J. K., Olaniyi, O. M., & Olalere, M. (2021). Blockchain technology in

IoT systems: current trends, methodology, problems, applications, and future directions. *Journal of Reliable Intelligent Environments*, *7*(2), 115-143.

Bakhshi Kiadehi, K., Rahmani, A. M., & Sabbagh Molahosseini, A. (2021). A fault-tolerant architecture for internet-of-things based on software-defined networks. *Telecommunication Systems*, *77*, 155-169.

Bhavana, K., Nekkanti, V., & Jayapandian, N. (2019, August). Internet of things enabled device fault prediction system using machine learning. In *International Conference on Inventive Computation Technologies* (pp. 920-927). Cham: Springer International Publishing.

Devi, S. K., Thenmozhi, R., & Kumar, D. S. (2024, March). Self-Healing IoT Sensor Networks with Isolation Forest Algorithm for Autonomous Fault Detection and Recovery. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 451-456). IEEE.

Guo, H., Zheng, Y., Li, X., Li, Z., & Xia, C. (2018). Self-healing group key distribution protocol in wireless sensor networks for secure IoT communications. *Future Generation Computer Systems*, *89*, 713-721.

Lan, Z. (2023). A Comprehensive Review of Fault-Tolerant Routing Mechanisms for the Internet of Things. *International Journal of Advanced Computer Science and Applications*, *14*(7).

Li, S., Oikonomou, G., Tryfonas, T., Chen, T. M., & Da Xu, L. (2014). A distributed consensus algorithm for decision making in service-oriented internet of things. *IEEE Transactions on Industrial Informatics*, *10*(2), 1461-1468.

Luntovskyy, A., & Globa, L. (2019, June). Performance, reliability and scalability for IoT. In *2019 International Conference on Information and Digital Technologies (IDT)* (pp. 316-321). IEEE.

Mezquita, Y., Casado, R., Gonzalez-Briones, A., Prieto, J., Corchado, J. M., & AETiC, A. (2019). Blockchain technology in IoT systems: review of the challenges. *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, 2516-0281.

Sahoo, S. S., Veeravalli, B., & Kumar, A. (2016, September). Cross-layer fault-tolerant design of real-time systems. In *2016 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)* (pp. 63-68). IEEE.

Uppal, Mudita, et al. "Cloud-based fault prediction using IoT in office automation for improvisation of the health of employees. " Journal of Healthcare Engineering 2021 October18,2021,Volume 2021-ArticleID 8106467 | https://doi.org/10.1155/2021/8106467

Terry, Doug. "Toward a new approach to IoT fault tolerance." Computer 49.8 (2016): 80-83. Computer (Volume: 49, Issue: 8, August 2016) 10.1109/MC.2016.238