RESEARCH ARTICLE

SAMRIDDHI Volume 13, Issue 1, 2021 Print ISSN: 2229-7111 Online ISSN: 2454–5767

# Fault-tolerance System Design in the Internet of Things (IoT) Network with Blockchain Validation

Rajesh Kumar Sharma[1*], Ravi Singh Pippal[1]

Department of Computer Science & Engineering RKDF University, Bhopal, Madhya Pradesh, India

## Abstract

An Internet of Things (IoT) network contains huge heterogeneous sensing devices, architectures, and protocols. In this extensive IoT network, fault detection and management is a critical and time-consuming task. In this paper, a fault-tolerance system is proposed for the Internet of Things network using Blockchain integrity and security validation method, and this network will detect faults and provide solutions automatically to maintain the efficiency of the network. Fault-tolerance automation creates a significant impact in the extensive IoT network for its sustainability. The outcome presented in this paper shows that the blockchain-based network is highly fault-tolerant as compared to the centralized and cryptographic method-based network.

**Keywords:** Internet of Things, Blockchain, Fault-Tolerance, IoT Network

*SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology* (2021); DOI: 10.18090/samriddhi.v13i01.10

## Introduction

IoT is the internal/external communication of intelligent elements via the internet to provide intelligent services.[1] A dependableIoT system should provide reliable and fault-free services. A fault is a defect within the hardware or software systems that impacts the correct functionality. It is tough to establish a pattern for fault-tolerance in IoT since the IoT devices are heterogeneous, highly distributed, poweredon battery, relied upon wireless communication, and affected by scalability. The dispersion of IoT devices causes the entire system to suffer from, e.g., server crashes, server omission,incorrect response, and arbitrary failure. The wireless and battery dependency makes the IoT devices barely recoverable.Furthermore, being exposed to new devices and services impacts the system's performance.[2]

Although the IoT was innovated more than one decade ago, the researchers and industrial communities are still tryingto define its different aspects and Quality of Services (QoS), such as fault-tolerance. Hence, this research aims to identify and classify the domain state of the art and highlight the methods, techniques, and architectures that are potentially suitable to model a fault-tolerance IoT. For achieving thisgoal, a systematically mapped analysis and study have been performed. The primary analysis has been selected based on real inclusion and exclusion criteria and deep analysis.[3]

Typically, IoT infrastructures communicate through a central node or gateway connecting sensors, controllers, and the outside. However, this represents failure at a single point diminishes the availability and reliability required by critical applications such as health monitoring, cybersecurity in infrastructures, or personal safety.[4,5] The state-of-the-art protocols related to IoT and WSN applications have been mainly designed to improve the performance and hierarchy of networks. For instance, the improvements studied focus on automating the management and maintenance of tasks and increasing robustness under failures (e.g., electrical or communication). Thus, third-party management protocols (e.g., SNMP) monitor the node status and send warning messages. Moreover, a local self-recovery mechanism based on flash memories to prevent data transfer and network load. Several ways to avoid communication loss between a cluster and the outside were addressed, where the gateway is selected accordant to battery levels. Also, it is a solution to detect failures (e.g., low energy thresholds) for this purpose and manage gateways locally to avoid loss of communication of a WSN using virtual cells or groups of nodes.[6] Similarly, a cluster-head structure consisting of cell-head nodes is organized to communicate with a base station depending on

**Corresponding Author:** Rajesh Kumar Sharma, Department of Computer Science & Engineering RKDF University, Bhopal, Madhya Pradesh, India, e-mail: rajeshsharma.ercs@gmail.com.

**How to cite this article:** Sharma, R.K, Pippal, R.S. (2021). Fault-Tolerance System Design in the Internet of Things (IoT) Network with Blockchain Validation. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology,* 13(1), 53-58.

**Source of support:** Nil

**Conflict of interest:** None

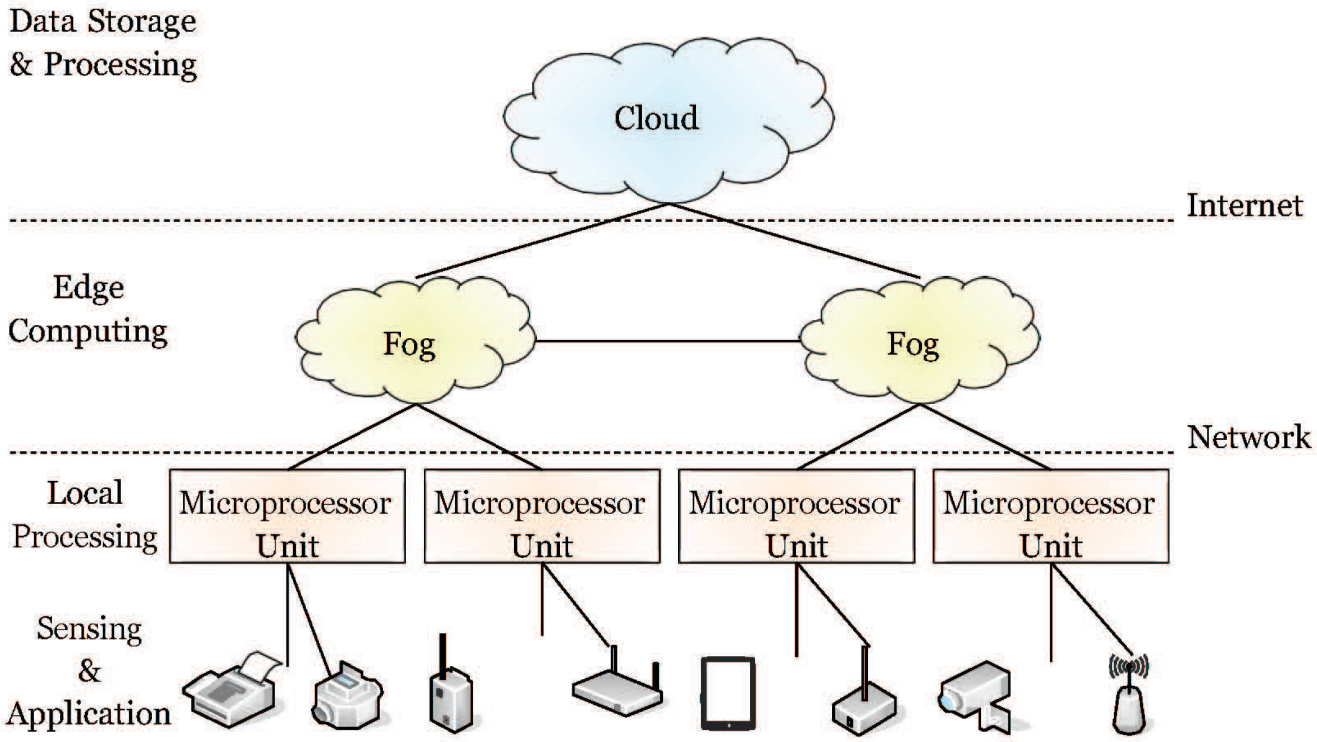

**Fig. 1:** Architecture of IoT

the sensors' energy. Moreover, the works focus on restoring the communication and retrieving information between a node and its gateway designating new routes through backup clusters.[7,8]

## Internet of Thing (Iot) Architecture

IoT applications typically consist of software components, including perception, data processing, and storage and actuation, which are distributed across the network as presentedin Figure 1. Most of the IoT networks focus on fault-tolerant data transmission and analysis, an architecture based on the subsequent data processing and storage modeling characteristicsare defined:

**Distribution:** This aspect specifies whether data analysissoftware should be deployed on a single node or sev- eral nodes distributed across the IoT system. In other words, distribution is referred to the deploymentof the IoT processing and storage software to hardware. By using a distributed style, the latency getsreduced due to data traffic and bandwidth consumption minimization. Such rapid response time facilitates real-time and fault-tolerant IoT applications. Furthermore, in distributed systems, faulty processing, and storage still holds IoT systems available since another one can replace the faulty component.

**Localization:** Depending on data size and required analysis complexity, processing and storage can be executed locally or remotely. Here is the point at which centralizedcloud and distributed edge and fog concepts become relevant. The advantage of using a central cloud is that process on a cloud component facilitates long-term data processing and analysis for those systems that have no constraints on response time. For applications with massive processing and storage requirements, executing the powerful cloud task is the only solution. Fog nodes are the intermediate processing and storage, which bring a degree of cloud functionality to the network edge.Fog is not limited to performing on a particular device to be located between device edge and cloud freely. The analysis capacity of fog is lower than cloud, but it reduces a significant point of failure by shifting towards more than one computational component. However, fog only performs locally, so it does not haveglobal coverage over a major IoT system. It is worth mentioning that some IoT devices can perform simple processing and storage by themselves. Performingprocessing and storage on IoT device edge refers to computation capabilities embedded on a smart device to gather and analyze environmental data.

**Collaboration:** The aforementioned computation components may interact to form and empower IoT services. This collaboration may appear as a level of information sharing, coordinated analysis and/or planning, or synchronized actuation. Each IoT sensor network may provide data for many collaborative data processing and storage components, both locally and remotely. Here the advantage is that if the local processing and storage node fails, local service is still in access.

## Faults Diagnosis Methods in IoT Network

The fault diagnosis method detects, identifies, and isolates the faulty IoT device, communication link, processing element, and system faults.[2] The primary fault model is presented in Figure 2.

All the elements of IoT devices can be classified into two primary ingredients,

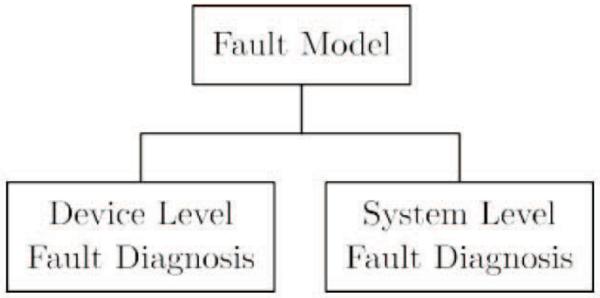

**Fig. 2:** Basic Fault Model

- The first category consists of nodes with a processor/ microcontroller (on-board), the storage sub-system (memory cards), and DC power supply units.
- The second category includes actuators and sensors.

Notably, all components from the first group are much more authentic and trust-able than the second. That means they have a much lower rate of failures. However, the simultaneous occurrence of microprocessor and sensor faults can not be isolated. The faulty nodes and their associated sensors must be examined, treated, and removed from the network. The communication links are assumed to be faulty at theaccess layer of the entire sensor network, and communication nodes, sink or base stations, gateways are also assumed tobe faulty[9]. The level of the fault diagnosis model is categorized as:

**Sensor Level Fault Diagnosis:** Fault diagnosis is performed basically in two phases – firstly, processing nodes such as (microprocessor/microcontroller) diagnosisin that the processing elements reliability states are diagnosed and the secondly, sub-system level phase where hardware performance and condition of each the sensor/actuator is found out. By sending the similar input into the pairs of nodes, the diagnosis is performed, and their responses are compared. The user may be capableof claiming the fault-free status of the nodes based on the collective outcomes of comparisons in the secure andfault-tolerant network.

- **System-Level Fault Diagnosis:** At the system level, the communication nodes and links are diagnosed, which haveto be performed. At the system level, communication links faulty, and communication nodes are diagnosed based on distributed agents.

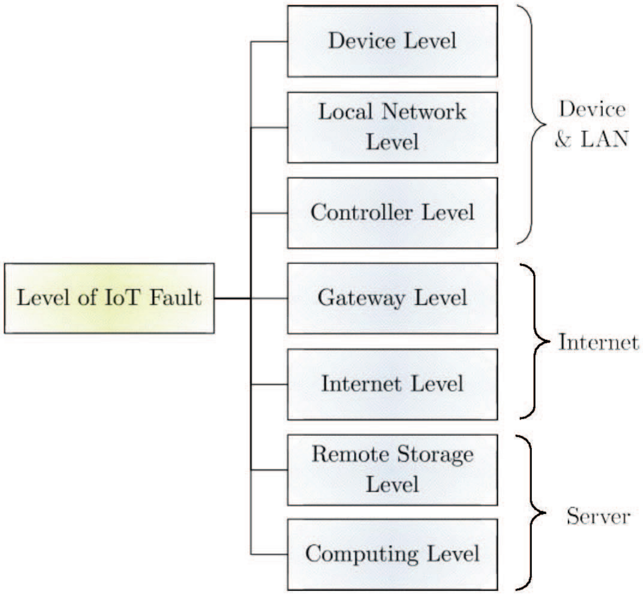

**Fig. 3:** Level of Fault in Internet of Things

## IoT Fault-Tolerance Open Issues

Internet of things, as next-generation technology, must be maintainable, reparable, scalable, and fault-tolerant. Although for some IoT applications (home automation, smart industry), fault tolerance transparency works comfortably; however, it is not ideal in many cases (surveillance, defense). Some IoT networks become failures (inherent faults); therefore, a failure-free network is required. Broken or weakness in components, malfunctioning, partial breakdown, and security leakage in IoT devices are common reasons for fault occurrence or failure of the network.[10]

Figure 3 represents the different fault levels in the entire IoT network from the device to the server. IoT networks may fail due to faults in the local device or network level, internet level, and server level. Once the fault occurs, the network becomes in-operational, so the IoT system must be completely fault-tolerant, and it must be an integral part of the IoT system.[11]

The challenging open issues regarding IoT fault-toleranceis summarized as:

- Modern smart applications and their underlying platforms.
- Cost-effectiveness for fault-tolerant IoT network.
- Effect of environmental conditions on the network.
- The interplay between fault tolerance and application semantics in an IoT world
- Reliability in a world of devices with widely ranging characteristics, including functionality, failure rates, and recovery modes
- Human expectations for fault tolerance might vary across devices.

## Related Work

Various literature presents specific strategies to diagnose faults in the IoT network. Various models, frameworks, architectureshave their advantages and also have limitations. Boudaa and Belouadah[12] presented a simple fault-tolerant and energy-efficient reservation-based DAMA protocol for per-mutation routing protocol for the single-hop wireless network of things. Cheraghlou *et al*. a new architecture of fault tolerance, which simultaneously uses proactive and reactive policies, wasthe goal of this research. The proposed architecture covers fault-tolerance on the quintuple phases, which consisted of fault forecasting, fault prevention, fault detection, fault separation, and fault recovery. The primary reason to completely address each of the five phases of fault tolerance by the architecture mentioned above, while simultaneously using all ofthe proactive and reactive policies in this architecture.

Dom´ınguez *et al*.[13] proposed a robust fault-tolerant performance system for resilient IoT- based infrastructures. IoT infrastructures communicate through a central node that connects sensors, actuators, andthe outside. When said node fails, it compromises reliability, endangering the entire network. To avoid it, protocols must automate the network management and provide high toleranceto failures (e.g., electrical, communication, etc.). With this aim,this paper proposes a protocol that autonomously managesa high availability node-based structure for critical WSN applications based on a microcontroller.

Grover and Garimella[14] proposed work to improve fault tolerance and reliability of edge computing with the help of an intelligent agent. The given architecture provides solutions for the possible faults at all levels in the cloud-hierarchy. To deal with any fault or issue, the proposed concept works with both reactive and proactive solutions. Their outcomes also show the efficiency of their defined architecture.

Hasan and Al-Turjman *et al*.[15] proposed a bio-inspired particle multi-swarm optimization (PMSO) strategy to construct, recover and select k-disjoint multipath routes. Two Position information in terms of personal-best position and the global positioning system is established in the form of velocity updates to enhance the performance of the routing algorithm. They assessed objective functions that analyze the average energy expenditure and average in-network delay to validate this strategy.

For supporting application developers to the fault-tolerant program and mechanism of IoT devices, Hu *et al*.[16] proposeda programming framework. The developers of this applicationcan follow this framework to determine and control the exception handling process in the task execution. Within the fault-tolerant enabled software architecture, the exception handling can be cooperated for recovering task execution during the unconditional error state. To improve the efficiency of recovery execution, the mechanism of synchronized state maintenance properly synchronizes the state record for maintaining theconsistency of each device in a similar local wireless sensor network. To evaluate the proposed programming framework, they used a case study to communicate strategy underthe situation of some failure Bluetooth and WiFi components among several nodes. The experimental results observed that the failure recovery and improvement mechanism implemented in their programming framework offers some benefits: concurrently with the other sensor nodes, each node can detect various errors that occurred by themselves through exception handling. Also, it can recoverby itself depending on the performance of the state table ofthe sensor node with the minimum workload on exchanges of messages among nodes.

Javed *et al*.[17] proposed a federated Edge-Cloud architecture, IoTEF, for IoT/CPS applications by adapting our earlier CEFIoT layered design. It uses the same state-of-the-art cloud technologies as CEFIoT, including Docker, Kubernetes, and Apache Kafka, and deploys them for edge computing. This new architecture has four layers:

- Application Isolation,
- Data Transport,
- Distributed OS, and
- Unified Federated Management layer.

Terry[18] presented a new approach to IoT fault-tolerance; however, for some IoT applications, transparent fault tolerancemay work well, but it may not be an ideal condition in all other cases.

## Proposed System Model

This section address the integrated network stability and robustness analysis of network design overhead. The integratednetwork stability is measured concerning changes in the area and the network structure and design latency. The network design processing time analysis is accomplished about network area designing, latency, and integration network stability. Based on the following equation, The integrated network stability is evaluated as to where,

$$NetStab_I = \overset{n}{\underset{i=1}{}} wi \frac{L_i}{Lmax_i} + \frac{A_i}{Amax_i} \quad (1)$$

NetStab$_I$ is the total integrated network stability and robustness of method for network configuration, the IoT network consists of the i$^{th}$ device to n$^{th}$. *L* denotes the total processing latency, A denotes the network area, $L_{max}$ denotes the maximum processing latency, and $A_{max}$ denotes the maximum area. *w* is a specific weight factor, and it is set to 0.5. The network is simulated using around 500 nodes with assuming centralized system, DES cryptography-based system, and Blockchain-based security system.

### Result Analysis

Figure 4 represents the fault-tolerance analysis of the Internet of Things network, which shows that the blockchain-based system presents high stability and robustness compared

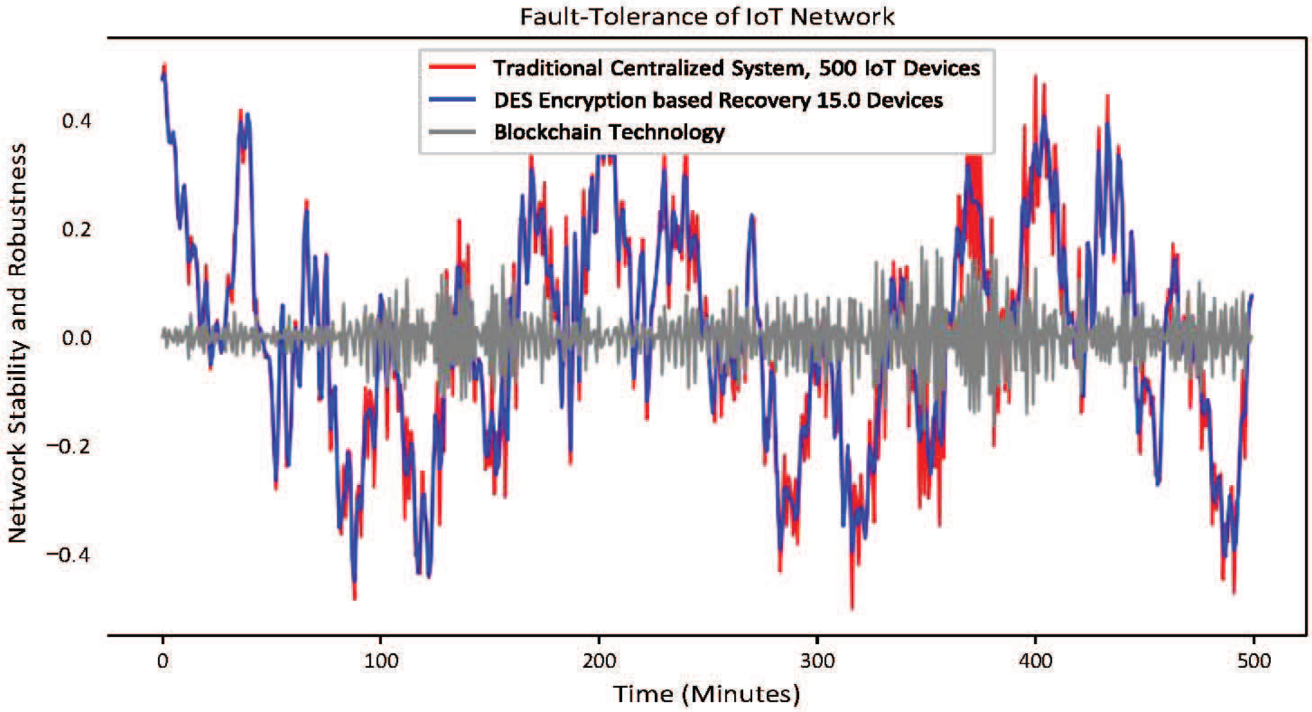

**Fig. 4:** Fault-Tolerance Analysis

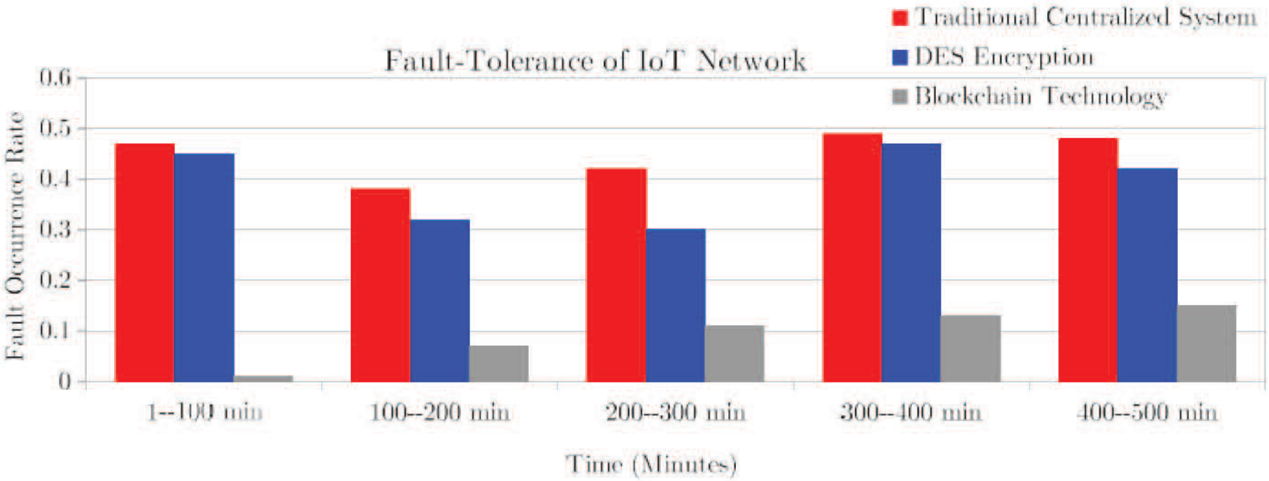

**Fig. 5:** Fault occurrence analysis

**TABLE I:** Result analysis (fault occurrence rate)

| *Time (min)* | *Fault Occurrence Rate* | | |
|---|---|---|---|
| | *Centralized (%)* | *DES (%)* | *Blockchain (%)* |
| 0 – 100 | 0.47 | 0.45 | 0.01 |
| 100 – 200 | 0.38 | 0.32 | 0.07 |
| 200 – 300 | 0.42 | 0.30 | 0.11 |
| 300 – 400 | 0.49 | 0.47 | 0.13 |
| 400 – 500 | 0.48 | 0.42 | 0.15 |

to the traditional centralized network and DES encryption algorithm. Figure 5 represents the maximum fault occurrence rate analysis for a centralized system, DES encryption algorithm, and blockchain. Table I represents the fault occurrence rate of simulation analysis for centralized, DES, and Blockchain-based networks. From the simulation result presented in graph and table shows that blockchain-based network is highly fault-tolerant and the fault occurrence rate is also low using this system.

Device-to-device communication in IoT networks is at the center of a system in designing and sharing information in anIoT ecosystem, with the latter being stored in the cloud.

The information retrieved from the IoT ecosystem is to be sharedin a secured and reliable framework using blockchain-based validation. Efficient cryptographic algorithms can be used to encrypt information, but it is not a good fault-tolerant system. Soblockchain-based security system provides high stability and robustness of the network.

## Conclusion

An Internet of Things (IoT) network contains a vast collection of heterogeneous sensing devices, architectures, and protocols. In this extensive IoT network, fault detection and management is a critical and time-consuming task. In this paper, a fault-tolerance system is proposed for the Internet of Things using blockchain integrity, and the security validation method is superior to the other method as presented in the simulation result, this the network detects faults and provides solutions automatically to maintain the efficiency of the network. Fault-tolerance automation create a significant impact in the large IoT network for its sustainability.

## References

[1] H. Muccini and M. T. Moghaddam, “Iot architectural styles,”in *Software Architecture*, C. E. Cuesta, D. Garlan, and J. Pérez, Eds. Cham: Springer International Publishing, 2018, pp. 68–85. doi: https://doi.org/10.1007/978-3-030-00761-4 5

[2] Z. Zieliski, J. Chudzikiewicz, and J. Furtak, *An Approach to Integrating Security and Fault Tolerance Mechanisms into the Military IoT*. Cham: Springer International Publishing, 2019, pp. 111–128. doi: https://doi.org/10.1007/978-3-030-02807-7 6

[3] M. S. Mohd Hafizi, N. A. Mat Leh, N. A. Kamarzaman, and N. H. Ishak, “Developing a monitoring system for trippingfault detection via iot,” in *2018 9th IEEE Control and System Graduate Research Colloquium (ICSGRC)*, 2018, pp. 110–115. doi: https://doi.org/10.1109/ICSGRC.2018.8657555

[4] T. Kung, C. Hung, Y. Teng, J. Hung, and L. Hsu, “Onthe robust approach to data inconsistency detection of sensor networks,” in *2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2016, pp. 425–429. doi: https://doi.org/10.1109/IMIS.2016.71

[5] A. Xenakis, A. Karageorgos, E. Lallas, A. E. Chis, and H. Gonza’lez-Ve’lez, “Towards distributed iot/cloud based fault detection and maintenance in industrial automation,” *Procedia Computer Science*, vol. 151, pp. 683–690, 2019. doi: https://doi.org/10.1016/j.procs.2019.04.091

[6] S. A. Viktoros, M. K. Michael, and M. M. Polycarpou, “Compact fault dictionaries for efficient sensor fault diagnosis in iot-enabled cpss,” in *2020 IEEE International Conferenceon Smart Internet of Things (SmartIoT)*, 2020, pp. 236–243.doi: https://doi.org/10.1109/SmartIoT49966.2020.00042

[7] A. K. Gupta and R. Johari, “Iot based electrical device surveillance and control system,” in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019, pp. 1–5. doi: https://doi.org/10.1109/ IoT-SIU.2019.8777342

[8] M. Kurtulus, F. Irgi, M. Namdar, A. Basgumus, and R. Temirtas, “Internet of things based predictive mechanical fault detection system,” in *2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, 2020, pp. 1–7. doi: https://doi.org/10.1109/ISMSIT50672.2020.9255004

[9] T. Dang, M. Tran, D. Le, V. V. Zalyubovskiy, H. Ahn, and H. Choo, “Trend-adaptive multi-scale pca for data fault detection in iot networks,” in *2018 International Conferenceon Information Networking (ICOIN)*, 2018, pp. 744–749. doi: https://doi.org/10.1109/ICOIN.2018.8343217

[10] S. JKR and Bhupathi, “Enhancing fault tolerance of iot networks within device layer,” *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 2, pp. 491–509, 02 2020.

[11] C. Seabra, M. A. Costa, and M. M. Lucena, “Iot based intelligent system for fault detection and diagnosis in domestic appliances,” in *2016 IEEE 6th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, 2016, pp. 205– 208. doi: https://doi.org/10.1109/ICCE-Berlin.2016.7684756

[12] A. Boudaa and H. Belouadah, “Fault-tolerant communication for iot networks,” in *Information Systems and Technologies to Support Learning*, ÁRocha and M. Serrhini, Eds. Cham: Springer International Publishing, 2019, pp. 245–255. doi: https://doi.org/10.1007/978-3-030-03577-8 28

[13] J. M. Lozano Dom´ınguez, T. d. J. Mateo Sanguino, and M. J. Redondo Gonza’lez, “Evaluation of a robust fault-tolerant mechanism for resilient iot infrastructures,” in *Broadband Communications, Networks, and Systems*,

[14] V. Sucasas, G. Mantas, and S. Althunibat, Eds. Cham: Springer International Publishing, 2019, pp. 3–12. doi: https://doi.org/10.1007/978-3-030-05195-2 1 \

[15] J. Grover and R. M. Garimella, “Reliable and fault-tolerantiot-edge architecture,” in *2018 IEEE SENSORS*, 2018, pp. 1–4. doi: https://doi.org/10.1109/ICSENS.2018.8589624

[16] M. Z. Hasan and F. Al-Turjman, “Optimizing multipath routing with guaranteed fault tolerance in internet of things,” *IEEE Sensors Journal*, vol. 17, no. 19, pp. 6463–6473, 2017. doi: https://doi.org/10.1109/JSEN.2017.2739188

[17] Y.-L. Hu, Y.-Y. Cho, W.-B. Su, D. S. Wei, Y. Huang, J.-L. Chen, I.-Y. Chen, and S.-Y. Kuo, “A programming framework for implementing fault-tolerant mechanism in iot applications,” in *Algorithms and Architectures for Parallel Processing*, G. Wang, A. Zomaya, G. Martinez, and K. Li, Eds. Cham: Springer International Publishing, 2015, pp. 771–784. doi: https://doi.org/10.1007/978-3-319-27137-8 56

[18] A. Javed, J. Robert, K. Heljanko, and K. Fra¨mling, “Iotef: A federated edge-cloud architecture for fault-tolerant iot applications,” *Journal of Grid Computing*, vol. 18, no. 1, pp. 57– 80, Mar 2020. doi: https://doi.org/10.1007/s10723-019-09498-8

[19] D. Terry, “Toward a new approach to iot fault tolerance,” *Computer*, vol. 49, no. 8, pp. 80–83, 2016. doi: https://doi.org/10.1109/MC.2016.238