RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 06, Issue 09 September

Check for updates

http://dx.doi.org/10.47392/IRJASH.2024.038

Comparative Study of Conventional and New Approaches for Attaining an Effective Fault Tolerance in IoT

J. Rajendran

Associate Professor & Head, Dept. of Computer Science, The Madura College, Madurai, Affiliated to Madurai Kamaraj University, Madurai, India.

Emails: *jrajendranmc@gmail.com*

Article history

Received:05 September 2024
Accepted: 12 September 2024
Published:16 September 2024

Keywords:
Internet of Things (IoT); Fault tolerance; IoT-enabled devices

Abstract

Fault Tolerant IoT devices are the latest products that received more hype from the general public. This sudden hype for fault-tolerant IoT devices is due to some occurrence of faults in the IoT applications which results in the malfunctioning of the entire system. At Present Fault-tolerant IoT devices are expensive, but people prefer them, for better living. In recent years, there has been discussion around the world about the enhancement of fault-tolerant IoT devices as they have become old. The conventional way of attaining fault tolerance is the employment of majority consensus and triple modular redundancy. These techniques are more commonly utilized by people who wish to achieve fault tolerance. As the years passed, the users of fault-tolerant IoT devices desired to upgrade the whole mechanism by adopting fresh techniques. Fault tolerance is achieved by applying a set of analysis and design techniques to create systems with dramatically improved dependability. As new technologies are developed and new applications arise, new fault tolerance approaches are also needed. In the early days of fault-tolerant computing, it was possible to create custom hardware and software solutions from scratch. However, with the current technology, chips contain complex, highly integrated functions, requiring hardware and software to meet various standards in order to be economically feasible. This paper presents a survey and a comparative study on fault tolerance provided in a variety of ways, then suggests an innovative scheme for attaining fault tolerance in IoT.

1. Introduction to Influencer Marketing

Fault tolerance has been the subject of substantial research in computer science. Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of some of its components. It is related to availability, reliability, safety, and maintainability [1]. Reliability and availability have become increasingly important in today's computer-dependent world. The Methods for coping with the existence and manifestation of faults can be classified into three families. They are fault avoidance, fault removal, and fault tolerance. In many applications where computers are used, outages or malfunctions can be expensive, or even disastrous. To achieve the needed reliability and

availability, we need fault-tolerant computers [2]. They can tolerate faults by detecting failures and isolating defect modules so that the rest of the system can operate correctly (Figure 1).

2. Fault in IOT Network

The latest technology which is commonly termed as the Internet of Things should be scalable, maintainable, fault-tolerant, and repairable. Even though there is fault tolerance transparency in some IoT applications which works well, there are occurrences of faults in some IoT networks. A fault-free network is a must for the requirements of this current world [3-5]. The faults in IoT networks are commonly due to security leakage, broken elements, weak components, partial breakdown, and malfunctioning (Moghaddam, Mahyar Tourchi, & Henry Muccini, 2019). The figure below presents the different levels of fault in the IoT network.

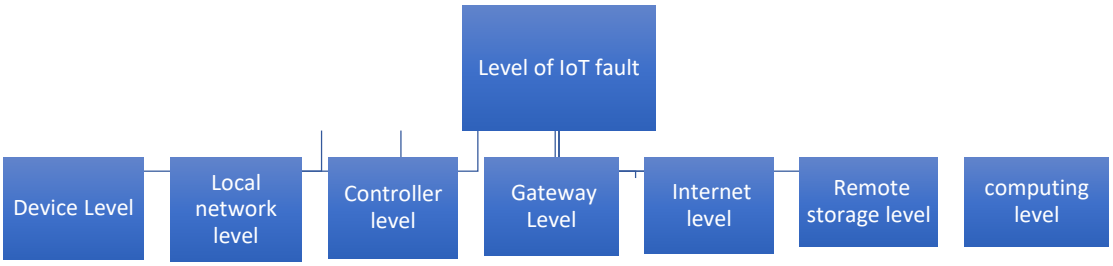

Figure 1 Different Levels of Fault

2.1 Diagnosis of faults in IoT Network

The techniques used for fault diagnosis detect the fault in the IoT network and separate the defective processing component, device, system faults & communication link. The components of IoT devices are classified into two basic categories. The first category has nodes with DC power supply units, processors or microcontrollers, and storage sub-systems [6]. The second category has sensors and actuators (Uppal, Mudita, et al., 2021). It is generally observed that the first category of elements in IoT devices have a low rate of failures as they are quality & trustable components. Isolation of similar fault incidence in sensor & microprocessor cannot be done. The nodes and the linked sensors that are faulty should be identified, isolated, and detached from the network. At the access layer of the complete network, there is an assumption of fault in communication links, gateways, communication nodes, and base stations (Grover, Jitendcr, and Rama Murthy Garimella, 2018). The common fault model is given in the flowchart below. Diagnosis is conducted in two types which are displaced in the chart (Figure 2).

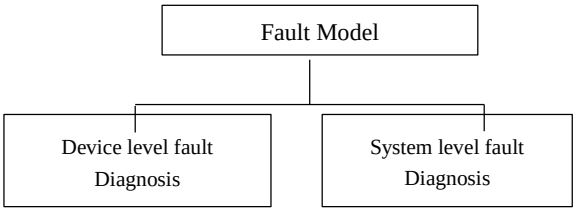

Figure 2 Fault Diagnosis Level

Device Level Fault Diagnosis – The device level fault diagnosis is performed in two phases. In the first phase, the diagnosis of the reliability state of processing components in the processing nodes like microcontroller or microprocessor is done [7]. In the second phase, the condition and performance of the hardware of each actuator or sensor are diagnosed. This phase is called the sub-system level phase. The diagnosis and the comparison of response are done by sending the same input into node pairs. The result of this comparative outcome in the fault-tolerant and secure network becomes the base for the fault-free claim of the node status (Karthikeya, Surabhi Abhimithra, et al 2016).

System Level Fault Diagnosis – The diagnosis of communication links and nodes at the system level is performed. Based on the distributed agents, the faulty communication links and communication nodes at the system level are detected and isolated.

2.2 Importance of Fault-Tolerant IoT Network & The Current Issues

The entire IoT network may fail because of the fault at the server level or internet level or device & LAN level. The network becomes non-functional if a such fault occurs in the IoT system. Hence, the fault-tolerance is a much-needed feature in IoT networks. Most of the transparent fault-tolerant features work well but it is not the same in all cases. In smart home IoT applications, there are issues in fault-tolerant networks. For example, a lighting app

which is a basic smart home IoT application selects sensors that have accurate reports indicating the presence of a person (Casado-Vara, Roberto, et al., 2019). The application cannot choose a sensor without analyzing the report as it may activate the motion sensor in the wrong place in the room. The fault in the IoT device might cause the application to act incorrectly i.e. lighting the wrong place. The main issues in the fault tolerance feature are listed below [8-11].

- Cost-effectiveness of fault-tolerant IoT network
- Reliability of failure rates, functionality & recovery modes
- Latest smart applications & connected platforms
- Varied human expectations for fault tolerance
- Connection between application semantics in IoT network & fault tolerance
- Impact of environmental condition

2.3 Current Issues

Today's IoT applications utilize three different computation environments: sensors, edge, and cloud. Ensuring fault tolerance at the edge level presents unique challenges due to complex network hierarchies and the presence of resource-constrained computing devices. The following are the most important issues in the development of IoT applications [12].

- Security issues
- Development costs
- Reliability of hardware
- Ease of Integration
- Connectivity
- Quality control

Some of the activities may address these issues through proper analysis and performance. Regular updating of expertise in device management, allocating a budget for security solutions, researching the quality in terms of durability and reliability of the devices, and frequent updates and maintenance of both hardware and software will be the solution for these issues [13].

3. Methodology

Even though many methodologies have been explored through research and analysis, some procedures for implementing fault-tolerant systems in hardware and software have been established. This paper is a comparative study of the conventional ways and new approaches to attaining fault-tolerant IoT applications. Secondary data collection is employed in this study. The data is gathered from external sources like Google Scholar, IEEE journals, IEEE Xplore, ResearchGate, etc. The search strategy is presented in the above chart (Refer Table 1).

Table 1 Search Strategy

S. No	Author	Year	Title	Objective	Database	Keywords used
1.	Ravi Singh Pippal, Rajesh Kumar Sharma,	2021	Fault-tolerance System Design in the Internet of Things (IoT) Network with Block chain Validation	A fault-tolerant system is proposed to detect and rectify the faults in the networks	Google Scholar	IoT, Fault tolerance
2.	Perigisetty Vedavalli, Deepak. Ch	2020	Enhancing Reliability and Fault Tolerance in IoT	Determining ways to enhance reliability and fault tolerance	IEEE	IoT, Fault tolerance
3.	Doug Terry	2016	Toward a New Approach to IoT Fault Tolerance	Analyzing new approach regarding IoT fault tolerance	IEEE	IoT, Fault tolerance
4.	Asad Javed	2022	A Scalable and Fault-Tolerant IoT Architecture for Smart City Environments	Analyzing the efficacy of fault-tolerant IoT applications in smart cities	Google Scholar	IoT, Fault tolerance
5.	Abhay Agrawal, Devendra Toshniwal	2021	Fault Tolerance in IoT: Techniques and Comparative Study	Examining the current fault tolerance techniques employed in IoT	Research Gate	IoT, Fault tolerance

4. Findings

4.1 Conventional Way of Achieving Fault Tolerance

The most common way to attain fault tolerance is the employment of majority consensus and triple modular redundancy. The device is built with three networks functioning in parallel which allows the device to survive any fault in software or hardware (Sharma, Rajesh Kumar, and Ravi Singh Pippal, 2021). For example, in lighting applications, IoT devices, three bulbs, three internet routers, three motion sensors, and three cloud providers are employed. Even though this system is efficient in functioning, there are some shortcomings. For example, IFTTT supports the code with single "if" & "then" actions [14]. Smart Things enables users to write code that connects with any number of devices but there is a restriction to connect to only one Smart Things hub. There are limitations in the current IoT network. Some IoT applications support only a single hub per house.

4.2 New Approach for Achieving Fault Tolerance

The new approach suggests various schemes for attaining fault-tolerant IoT. They are listed below [15].

- If the motion sensors experience a hardware failure, then the motion sensor stops functioning. A majority consensus or three motion sensors is not required to address this issue. The new approach suggests that two sensors are sufficient to address this issue (Vedavalli, Perigisetty, & Ch Deepak, 2020).
- Different IoT devices can report the same incident. To detect the motion of a person, a video camera, motion sensor, microphone, or smartphone can also be used. The new approach suggests that notification from varied devices could be used instead of employing three instances of the motion sensor.
- There are various types of hubs. Two hubs are sufficient for fault tolerance rather than buying three instances of a special-purpose hub (Terry, Doug, 2016). Multiple hubs are available in smart refrigerators, voice assistants, TVs, and internet routers. The new approach suggests taking advantage of the existing hubs.
- There is an availability of diverse wide-area networking technologies. Wide-area networks could be employed to attain fault tolerance instead of relying on multiple internet routers. The latter is expensive and also ineffective as they share a single internet connection from the house. The new approach suggests utilizing the diverse wide-area networking technologies available (Javed, Asad, 2022).
- IoT devices receive signals of events, process them, and take action. These are event handlers without states. Any local govt is a soft state that can be regenerated like caching sensor values when the application is restarted. The new strategy contends that IoT applications as replicated state machines are less necessary and of little usefulness.
- IoT applications can respond to outside events after a delay. During the event processing, the device takes some time which goes unnoticed. There can be an occasional delay in the response of the smart application. According to the new methodology, other hubs should be able to identify any hub failures and resume your application if they cause it to respond slowly. The applications can continue processing external events after being restarted. (Agrawal, Abhay, & Devendra Toshniwal, 2021).

5. Suggestions

Based on the analysis, a comparative study of the procedures implemented in the conventional and new approaches for achieving good fault tolerance the following suggestions may be considered:

- Suggests that two sensors are sufficient to address the issue providing a triple modular redundancy idea
- Instead of providing separate hubs for the devices connected to the IoT network, Multiple-port hubs may be used.
- Instead of using LAN or MAN NW topology, Wide-area networks could be employed to attain fault tolerance instead of relying on multiple internet routers.
- As an innovative suggestion, a stack-based algorithm may be chosen to determine the protocol and data format based on the

information and its synchronization for any network topology with homogeneity.

Conclusion

Fault tolerance in IoT devices is in great demand in the current times as IoT applications become faulty sometimes. This paper describes the installation of IoT in home automation, as well as how IoT network faults manifest and are identified. This paper also discusses the importance of fault-tolerant IoT devices in the present times. The issues about the fault-tolerant application are analyzed. This study has adopted a comparative study in which the techniques used to enhance fault tolerance in IoT devices in conventional times and the present times are explored. This study presents new approaches to improve the fault tolerance of IoT devices. Yet, improvements can be possible if many different challenges and issues are considered in any of the technical approaches. Developing an improved model must be considered by IoT developers since services are generated and a huge amount of data is generated by IoT. Most of the fundamental concepts discussed here deal primarily with localized rather than system-wide fault tolerance. Localized strategies are easy to understand and apply. System-level fault tolerance requires considerable work.

References

[1]. Santoso, Freddy K., and Nicholas CH Vun. "Securing IoT for a smart home system." International Symposium on Consumer Electronics (ISCE). IEEE, August 2015 10.1109/ISCE.2015.7177843

[2]. Calinescu, Radu, and Felicita Di Giandomenico, eds. Software Engineering for Resilient Systems: 11th International Workshop, SERENE 2019, Naples, Italy, September 17, 2019, Proceedings. Vol. 11732. Springer Nature, 2019.

[3]. 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 October 18, 2021, Volume 2021 | Article ID 8106467 | https://doi.org/10.1155/2021/8106467

[4]. Karthikeya, Surabhi Abhimithra, J. K. Vijeth, and C. Siva Ram Murthy. "Leveraging solution-specific gateways for cost-effective and fault-tolerant IoT networking." 2016 IEEE Wireless Communications and Networking Conference. IEEE, 2016. 2016 IEEE Wireless Communications and Networking Conference 10.1109/WCNC.2016.7564811

[5]. Grover, Jitendcr, and Rama Murthy Garimella. "Reliable and fault-tolerant IoT-edge architecture." 2018 IEEE sensors. IEEE, 27 December 2018 10.1109/ICSENS.2018.8589624

[6]. Casado-Vara, Roberto, et al. “Distributed continuous-time fault estimation control for multiple devices in IoT networks.” IEEE Access 7 (2019): 11972-11984. IEEE Access (Volume: 7) 15 January 2019 10.1109/ACCESS.2019.2892905.

[7]. Sharma, Rajesh Kumar, and Ravi Singh Pippal. “Fault-Tolerance System Design in the Internet of Things Network with Blockchain Validation.” SAMRIDDHI: A Journal of Physical Sciences, Engineering, and Technology 13.01 (2021): 53-58. Vol 13 No 01) June 30 2021 https://doi.org/10.18090/samriddhi.v13i01.10.

[8]. Vedavalli, Perigisetty, and Ch Deepak. “Enhancing reliability and fault tolerance in IoT.” 2020 International Conference on Artificial Intelligence and Signal Processing (AISP). IEEE, 2020. 10-12 January 2020 10.1109/AISP48273.2020.9073174

[9]. 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

[10]. Agrawal, A., & Toshniwal, D. (2021). Fault Tolerance in IoT: Techniques and Comparative Study. Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146, 7(1), 49-52. Volume 7 No-1 2021https://doi.org/10.33130/AJCT.2021v07i01.011.

[11]. Colacovic A, Hadzialic M. Internet of things (IoT): a review of enabling technologies, challenges, and open research issues. Computer Networks. 2018; 144:17–39.

[12]. Fafoutis X, et al. A residential maintenance-free long-term activity monitoring system for healthcare applications. EURASIP J Wireless Communication Network. 2016.

[13]. Wikipedia. Fault-tolerant system,

http://en.wikipedia.org/wiki/Fault_tolerane
[14]. A Conceptual Framework for Systems Fault Tolerance,http://hissa.nist.gov/chissa/SEI_ Framework/framework_1. html
[15]. H. Ammar, B. Cukic, C. Fuhrman, and A. Mili Institute for Software Research Fairmont, WV 26554 USA. http://www.isr.wvu.edu.