International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I8P209

Volume 71 Issue 8, 102-118, August 2023

Original Article

Evaluation of Designing Techniques for Reliability of Internet of Things (IoT)

Khushwant Singh[1], Yudhvir Singh[2], Dheerdhwaj Barak[3], Mohit Yadav[4]

[1,2]*Department of Computer Science & Engineering, University Institute of Engineering and Technology, M.D.U, Rohtak, Haryana, India*
[3]*Department of Computer Science & Engineering, Vaish College of Engineering, Rohtak, Haryana, India*
[4]*Department of Mathematics, University Institute of Sciences, Chandigarh University, Gharuan, Mohali, India.*

[2]*Corresponding Author : dr.yudhvirs@gmail.com*

Received: 05 June 2023 Revised: 15 July 2023 Accepted: 22 July 2023 Published: 15 August 2023

Abstract *- Reliability of Internet of Things seeks out beneficial problems by presenting, resolving, and certifying them. Preparations are essential in addition to offering IoT responsiveness for the huge preparation of advances in the Internet of Things in all domains of society. The purpose of this study is to propose, examine, and explore surveys in planned works and their future rights based on the results of the IoT in this particular case. IoT's fundamental critical components are the usage of repeating devices that maximise the benefits of mobile phones, sensors, as well as actuators. Networking, along with other formula-based assessments, has amplified node-to-node connectivity at different levels in terms of IoT reliability. In the present study work, dependability metrics and models have undergone a rigorous assessment. Evaluation of work analysis and future prospective of different research articles in the detailed view of the reliability of the Internet of Things. A Novel model for reliability technique is being proposed, which qualifies the accuracy, and precision using various machine learning algorithms can be used. The measurement of reliability in the IoT provides several study avenues as a result of this thorough investigation. Despite the sensitive nature of the research field, studies that access models of IoT dependability are now communicating widely.*

Keywords *- Reliability, Internet of Things, Network reliability, Fault tree.*

1. Introduction

The Internet of Things (IoT) is a notion that describes how commonplace physical things, technologies, and appliances are connected to the internet and one another. These items, which often include sensors and actuators, have the ability to gather, share, and analyse data without the need for direct human involvement. The primary goal of IoT is to create a smart, interconnected network that enhances efficiency, automation, and convenience in various aspects of our lives.

The Internet of Things may be broken down into its essential parts and described in a few words. IoT devices form the foundation of the ecosystem. These can be anything from traditional household appliances, wearable devices, industrial machinery, smart home systems, vehicles, environmental sensors, and more. IoT devices require connectivity to transfer data. Common connectivity options include Wi-Fi, Bluetooth, Zigbee, cellular networks, and low-power wide-area networks (LPWAN).

IoT generates a vast amount of data. IoT systems rely on cloud computing, edge computing, or a combination of both to make sense of this data. Cloud computing involves processing data on remote servers, while edge computing manages information processing at the network's edge, where latency and bandwidth use are reduced. The collected data needs to be analysed to derive valuable insights. This analysis can lead to real-time decision-making, predictive maintenance, and optimisation of various processes. IoT solutions often provide user-friendly interfaces, such as mobile applications or web portals, to enable users to interact with and control their devices remotely. As IoT devices gather and share sensitive data, ensuring security and protecting user privacy are critical challenges. Implementing robust security measures is crucial to prevent unauthorised access and data breaches.

1.1. The Internet of Things

Predicting the exact state of the Internet of Things (IoT) by the year 2040 is challenging due to the rapidly evolving nature of technology and the many factors that can influence its growth. However, based on historical trends and potential advancements, we can make some speculative predictions about the state of IoT by 2040:

1.1.1. A.I. and Autonomous Systems

Machine learning and A.I. will be crucial Internet of Things components. IoT devices and systems will become

increasingly intelligent, capable of making autonomous decisions and adapting to changing conditions without human intervention.

1.1.2. Edge Computing Dominance

Edge computing will become the standard for processing data generated by IoT devices. This approach will significantly reduce latency, bandwidth requirements, and cloud dependency, making IoT systems more efficient and responsive.

1.1.3. Interoperability and Standards

With the continued growth of IoT, interoperability standards will become more mature and widely adopted. This will promote seamless communication and data exchange between different IoT devices and ecosystems.

1.1.4. IoT in Healthcare and Smart Cities

IoT will revolutionise healthcare, enabling remote patient monitoring, AI-powered diagnostics, and personalised treatments. Smart cities also leverage IoT technologies to enhance urban planning, transportation, and energy management.

1.1.5. Security and Privacy Measures

Given the exponential growth of IoT, cybersecurity will be a top priority. Advanced security measures will be implemented to protect IoT devices and networks from cyber threats, safeguarding user data and privacy.

1.1.6. Energy Efficiency and Sustainability

IoT devices will be designed to be highly energy-efficient, with more emphasis on sustainable power sources, leading to a reduced environmental impact.

1.1.7. Ethical and Social Considerations

As IoT becomes more pervasive, ethical and social considerations around data privacy, ownership, and responsible A.I. use will become paramount. Regulations and policies will be in place to address potential challenges. It is crucial to remember that these forecasts are theoretical and open to change depending on unanticipated technology advancements, social, economic, including political issues, as well as other elements that might influence the IoT's future. IoT in 2040 may look quite different from what we can now imagine. Gadgets scaling down, the cost of electronic parts, and the pattern towards remote interchanges are the three fundamental drivers for IoT [1-2].

Despite its numerous benefits, IoT adoption faces several challenges. Hackers can exploit IoT device vulnerabilities, leading to potential privacy breaches and cyber-attacks. With numerous IoT devices and platforms available, ensuring seamless communication and interoperability between different systems can be complex. The massive influx of data from IoT devices can overwhelm networks and servers, requiring efficient data management and analysis. A lack of uniform standards across IoT devices and protocols can hinder compatibility and hinder widespread adoption.

The Internet of Things is a cutting-edge network that has the potential to transform many facets of contemporary life. As IoT continues to advance, addressing security concerns, promoting standardisation, and maximising the potential benefits will be critical to realising its full potential[3-8].

1.2. Motivation and Goals

This paper evaluated all the different reliabilities in the Internet of Things based on hop by hop, end to end, including redundancy, packet loss delivery, and retransmission. There will be a discussion on a reliability review with future scope. Within its Interagency Technical Advisory Committee 1, ISO (International Organization for Standardization) has developed several standards specifically related to the Internet of Things (IoT). These standards aim to provide guidelines, specifications, and best practices to ensure interoperability, security, and efficiency in IoT deployments. Some of the key ISO standards for IoT are:

1.2.1. ISO/IEC 30141

This standard provides the IoT Reference Architecture (IoT R.A.) framework, which defines the general architecture for IoT systems. It offers a common basis for designing, building, and operating IoT solutions.

1.2.2. ISO/IEC 30145

This standard focuses on the security and privacy aspects of IoT. It provides guidelines and recommendations for securing IoT systems against potential threats and ensuring data privacy.

1.2.3. ISO/IEC 30118

This standard specifies a Lightweight M2M (LwM2M) protocol designed for efficient communication and management of IoT devices and platforms in constrained environments.

1.2.4. ISO/IEC 21823-3

This standard addresses the IoT Semantic Interoperability framework, which facilitates communication between heterogeneous IoT devices and systems by standardising data representations and semantics.

These ISO standards play a significant role in shaping the development and implementation of IoT solutions. They provide a framework for addressing key challenges and concerns related to interoperability, security, data management, and communication in IoT ecosystems. Organisations and developers involved in IoT projects can benefit from adhering to these ISO standards to ensure the success and reliability of their IoT deployments [9].

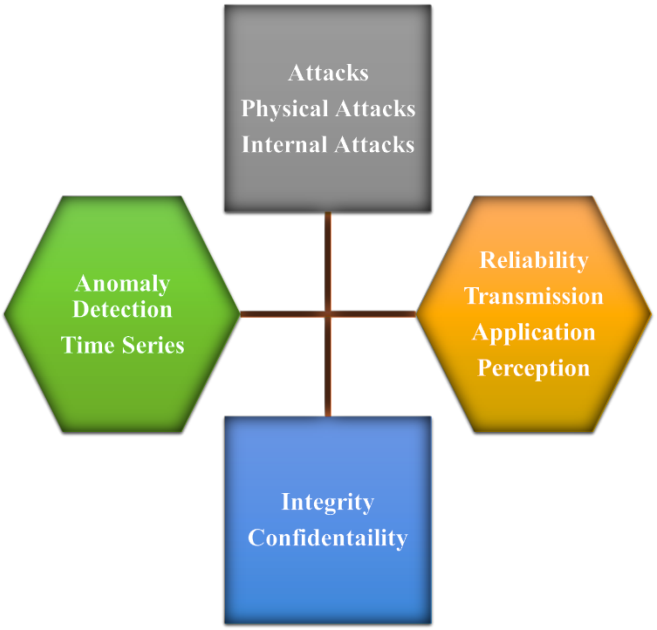

Fig. 1 Different issues facing of internet of things and their connection

IoT Reference Engineering, also known as IoT Reference Architecture or IoT Reference Model, is a standardised framework that provides a blueprint or guide for designing and implementing Internet of Things (IoT) systems. It offers a set of best practices, principles, and components to be used as a foundation for developing IoT solutions. The goal of IoT Reference Engineering is to promote interoperability, scalability, security, and reliability across different IoT implementations.

It is essential to understand that IoT Reference Engineering is not a one-size-fits-all solution. Each IoT project may require some level of customisation to meet specific use cases, business requirements, and technical constraints.

However, having a well-defined reference architecture can significantly expedite the development process and enhance IoT solutions' overall quality and reliability. Several organisations, standards bodies, and industry consortia have developed their own IoT reference architectures, such as IoT-A, Industrial Internet Reference Architecture (IIRA), and AWS IoT Reference Architecture. These can serve as valuable resources for IoT developers and engineers [10-11].

Exams with excessive innovation are now positioned to provide a network of people, things, and submissions across the internet. The Internet of Things (IoT) enables the development of various intelligent products and services by fusing information from both the physical and the digital realms. IoT devices will advance, according to the World Financial Gathering (WEF) observations about how the financial industry views the Internet of Things (IoT) [12-15].

1.3. Reliability Theory

The possibility of a framework meeting its expected appearance may be shown using reliability theory. The capacity of each segment to maintain continuous quality is taken into consideration while assessing a framework's dependability. The unchanging quality hypothesis was utilised by Yong-Fei et al. to evaluate the trustworthiness of the IoT. Five reliability characteristics and the application layer were offered for the observatory layer, the web, mobile devices, communications through satellites, and other systems. They estimated the overall IoT stable quality at 0.87 based on their suspicions. However, this should just be used as a barometer since the IoT is still rapidly growing, and the authors may not have considered all relevant elements. Using dependability theory, other IoT needs, such as Quality of Service as well as information for executives, may be handled. How trustworthy is the IoT data gathered? The reliability of the data from IoT sensors is impacted by issues such as information misfortune, noise, erroneous data, and data excess when a few sensors have predicted a similar item, according to Mama et al. [46]. The development of an accurate quality model for IoT data may result from taking each of these factors into account [16-17].

The Safe Community Awareness and Alerting Network (SCAN) is a concept that aims to enhance community safety and emergency response through the use of modern communication technologies. It is designed to provide timely and relevant information to residents and authorities during emergencies, disasters, and critical events [18].

Nevertheless, there are now a few programs dedicated towards IoT dependability planning and demonstration. The trustworthiness of the Internet of Things (IoT) can be demonstrated through various unique methods, which showcase the robustness and dependability of IoT systems. Here are some distinctive ways to display and evaluate IoT reliability:

1.3.1. Reliability Metrics Dashboard

Create a real-time reliability metrics dashboard that tracks key performance indicators (KPIs) related to IoT devices, network uptime, data transmission success rates, response times, and other relevant parameters. This dashboard provides a quick overview of the system's reliability at any given moment.

1.3.2. Failure Visualisation

Develop a visual representation of past failures or disruptions in the IoT system, such as a heat map or timeline, highlighting when and where incidents occurred. This helps identify patterns, trends, and areas that require improvement.

1.3.3. Simulation and Stress Testing

Conduct rigorous simulation and stress testing to subject IoT devices and the network to extreme scenarios and

evaluate how well they perform under adverse conditions. These tests can be used to measure the system's resilience and predict potential points of failure.

1.3.4. Redundancy in Action

Organise live demonstrations of redundant components in IoT devices or networks. Show how the system seamlessly switches to backup options in case of failures, ensuring continuous operation.

1.3.5. Energy Efficiency Tracking

Display energy consumption data for IoT devices and demonstrate how power-saving strategies, such as sleep modes or adaptive power management, contribute to extending device lifespans and reliability.

1.3.6. Real-time Data Accuracy Verification

Showcase how IoT devices and sensors validate the accuracy of the data they collect in real-time. This can include comparing sensor readings against known benchmarks or using redundant sensors to cross-validate data.

1.3.7. Data Integrity Demonstrations

Implement tamper-proofing measures on IoT devices and demonstrate their ability to maintain data integrity even in the face of malicious attempts to manipulate or compromise information.

Using unique and engaging methods to display IoT reliability demonstrates the system's effectiveness and instils confidence in stakeholders, customers, and end-users about the trustworthiness of the IoT solution.

Various researchers investigate IoT's administrative dependability, and it illustrates a contextual study utilising two subsystems that each continuously receive temperature and smoke data from a few sensors. An actuator accompanying warning is activated when these attributes go over a certain threshold. The paradigm, however, does not pay particular attention to failure situations.

Li et al. Describe a technique for evaluating the dependability of IoT devices that takes identification uniformity, transmission reliability, as well as preparation reliability into account [12]. Additionally, there is already a method for evaluating hardware and software reliability. The bulk of items or publications on the internet rely on setbacks, regardless of whether they happen alone or together, like numerous other events in our daily life. We could concur that the discontent structure has a certain possibility of appropriation without violating our point of agreement. Examining IoT metrics for accessibility and dependability necessitates considering the characteristics of IoT accessories and equipment [46–50]. The persistence function of "Internet of Things" devices, which are designed to identify and monitor physical objects, was also investigated in this research. The Internet of Things is distinct from the conventional internet in a number of important respects. For example, many use cases call for safety-critical requirements, layering must be energy-efficient, and most nodes need to be straightforward to build [51-55]. In order to address dependability issues spanning from packet delivery to network lifespan and application behaviour, the authors deliver specific design recommendations. They do this through the application of their earlier efforts and the formation of such networks [19-20].

$$R(t) = (1/(\alpha - 1)!)(\lambda t)^{\alpha - 1} e^{-\lambda t} \quad (1)$$

"For the purpose of trying to calculate an incident's average failure time or projected time to failure, we assume f(t) to be the probability density function preceding a failure. The expected value is then made clear as perceived in (2)".

$$E(t) = \int_0^\infty t f(t) dt \quad (2)$$

"The availability meter and the reliability metric are equal whenever an appliance does not need repair. The availability metric may be particularly checked if the failure rate is h while the repair rate is A(t) (3)".

$$A(t) = \frac{\mu}{\lambda + \mu\lambda} + \frac{\lambda}{\mu} e^{-(\lambda + \mu)t} \quad (3)$$

"If $t \to \infty$, (3) converts as the limiting probability intended for availability *MTR* = mean of repair = $1/\mu$.

Evaluating the reliability of IoT (Internet of Things) systems through Mean Time to Repair (MTTR) is an important aspect of assessing their performance and dependability. MTTR is a key metric used to measure the maintainability and availability of a system. It represents the average time taken to repair or restore a failed component or device in the IoT system after a failure occurs.

Here is how to evaluate IoT reliability using MTTR:

Identify Components and Record Failure Instances

Identify the critical components or devices in the IoT system that are prone to failure or significantly impact the overall system performance. Keep track of the failure instances of these identified components over a specified period. Note the time at which the failures occurred.

Measure Downtime and MTTR Calculation

For each failure instance, calculate the downtime, which is the time between the failure occurrence and the successful restoration of the failed component. Downtime includes the time required to detect the failure, diagnose the issue, and implement the repair or replacement. Add up all the downtime values and divide the total by the number of failure instances. This will give the Mean Time to Repair (MTTR) for the IoT system.

Analyse MTTR trends and comparison with SLAs

Analyse the MTTR trends over time to identify any patterns or improvements. A decreasing MTTR indicates that the system's maintainability is improving, while an increasing MTTR might highlight potential issues in the repair process. Compare the calculated MTTR with the Service Level Agreements (SLAs) or reliability targets set for the IoT system. SLAs typically define the maximum acceptable downtime for critical components, and MTTR should be within this limit.

Identify Improvement Opportunities

If the MTTR is higher than desired, investigate the root causes of the failures and downtime. Identify areas for improvement, such as enhancing maintenance procedures, optimising repair processes, or incorporating redundancy for critical components.

By evaluating the reliability of IoT systems through MTTR, organisations can proactively address maintenance and downtime issues, improve system performance, and ensure better availability of their IoT deployments. Regular monitoring of MTTR and continuous efforts to reduce it can lead to enhanced reliability and increased overall efficiency of IoT systems [21].

Evaluation of reliability data under the premise that the failure probability density function is represented by the usual Gamma function in equation (1). The discretisation of the gamma function results in two different failure concepts: the function of failure as well as the survival function.

Use the widely used Gamma probability density function technique to examine various IoT dependability and availability issues. A Markov model is a stochastic model used to analyse and predict the behavior of systems with a sequence of events that transition between different states over time. In the context of IoT reliability, a Markov model can be employed to assess the reliability and availability of IoT systems and devices as they transition between operational states. A Markov model will be used in later research to display the failure situations. [22]. A Markov model will be utilised in a later study to depict the events that lead to failure. (iii) Time complexity: For this structure currently in place, a building flowchart stipulates that the [22]. Figure 2 shows in what way an IoT framework is usually constructed.

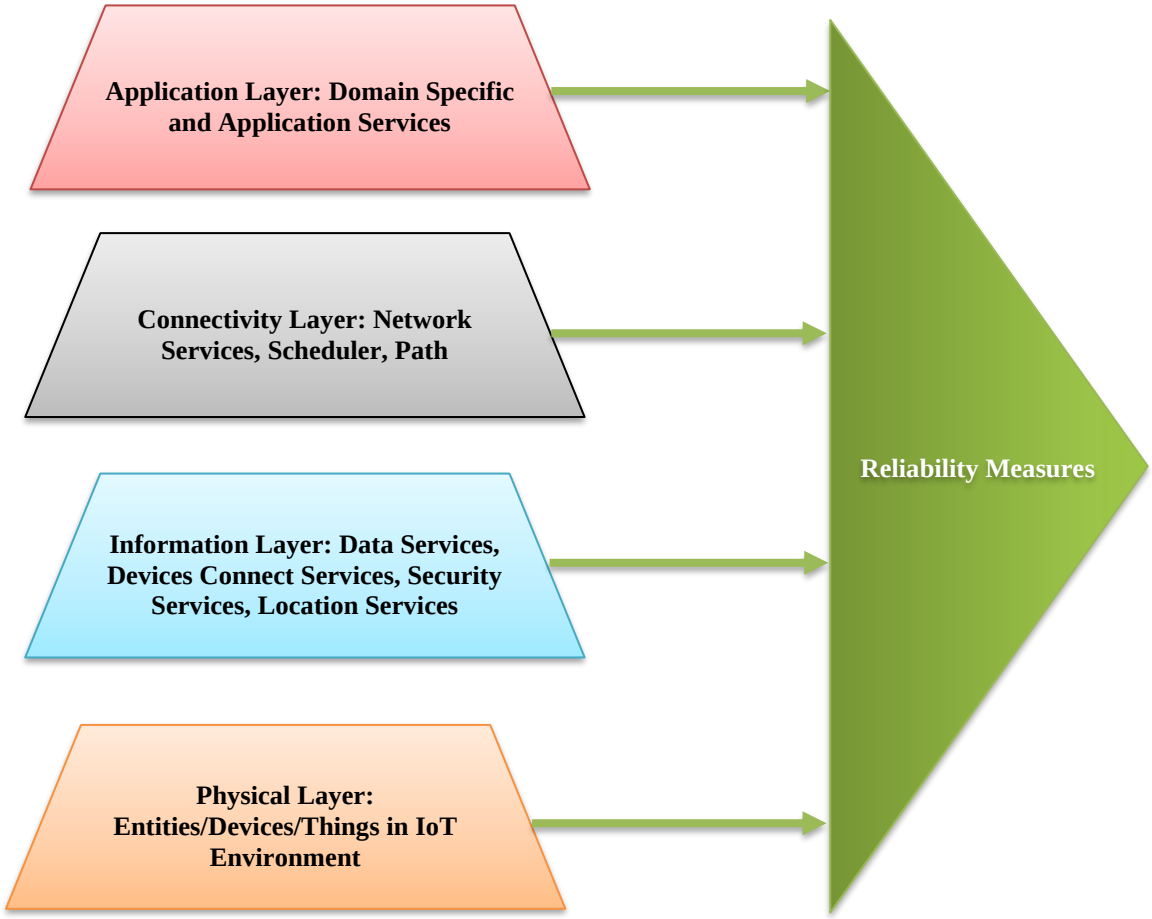

Fig. 2 Overview of the general internet of things framework

2. A Novel Model for IoT Reliability and IoT Reliability Framework

Dynamic Reliability Framework for IoT (DRF-IoT). The focus of this framework is to adaptively enhance the reliability of IoT systems in real-time based on dynamic conditions and requirements. Here are the key components of the DRF-IoT:

2.1. Dynamic Redundancy Management and Adaptive Security Mechanisms

The DRF-IoT incorporates dynamic redundancy management, which intelligently adjusts the level of redundancy in the IoT network based on the current operating conditions. During periods of high demand or potential failures, the framework will automatically increase redundancy to ensure fault tolerance. Conversely, it may decrease redundancy to optimise resource utilisation during stable conditions. The framework employs adaptive security mechanisms that continuously assess the risk landscape and adjust security protocols accordingly. This includes real-time threat detection, anomaly analysis, and automated responses to mitigate potential security breaches.

2.2. Context-Aware Interoperability and Intelligent OTA Updates

DRF-IoT emphasises context-aware interoperability, allowing IoT devices to dynamically adapt their communication protocols based on the context of their environment. This ensures seamless integration with heterogeneous IoT systems and improves overall reliability. The framework leverages machine learning and data analytics to schedule and intelligently deliver over-the-air (OTA) updates. These updates are optimised for each device, considering their unique characteristics, usage patterns, and available resources to minimise the risk of update-related failures.

2.3. Dynamic Data Integrity, Validation and Edge-Cloud Collaborative Processing

DRF-IoT employs dynamic data integrity and validation mechanisms that continuously monitor and verify data integrity as it traverses the IoT system. Any inconsistencies or anomalies are quickly detected and rectified to ensure accurate and reliable data transmission. DRF-IoT utilises a collaborative processing approach to enhance reliability and reduce latency, where data processing and analytics are distributed between edge devices and cloud infrastructure based on the data's criticality and real-time requirements.

2.4. Predictive Maintenance, Self-Healing, Continuous Monitoring and Real-Time Diagnostics

The framework integrates predictive maintenance algorithms to anticipate potential failures in IoT devices. In case of identified issues, self-healing capabilities are triggered to automatically address the problems or notify maintenance personnel, minimising downtime and service disruptions. DRF-IoT includes a comprehensive monitoring and diagnostics system that provides real-time insights into the health and performance of the IoT ecosystem. This allows proactive identification and resolution of issues before they escalate.

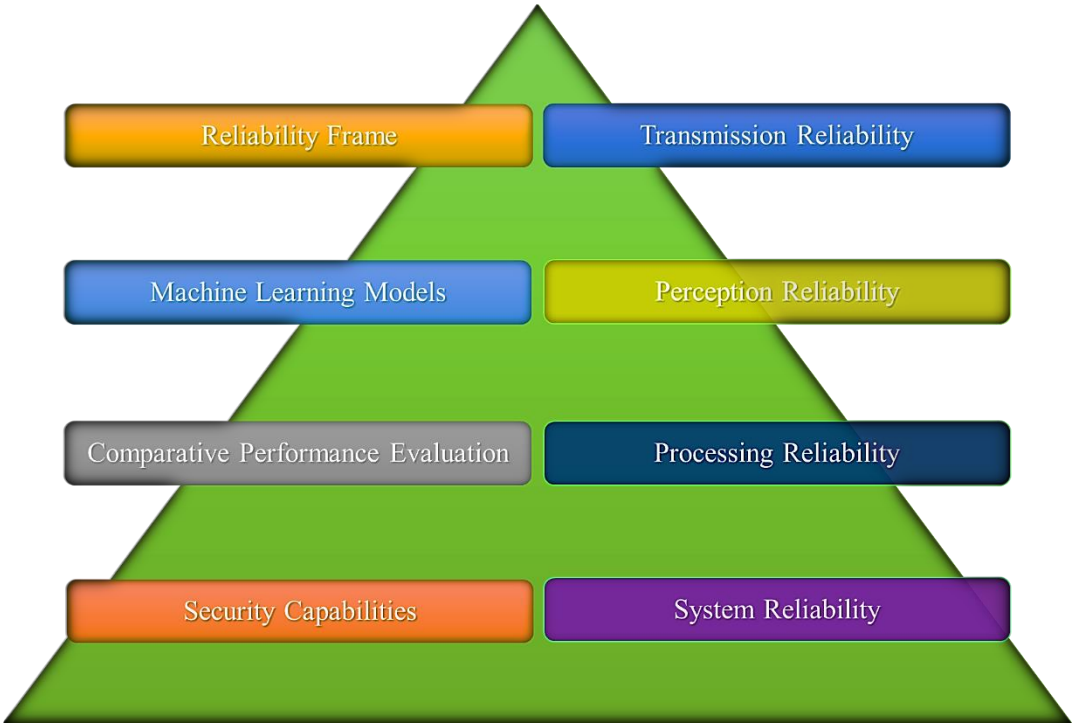

Fig. 3 A Novel model for reliability of the internet of things

2.5. Energy-Efficient Strategies, Learning and Adaptation

The framework employs energy-efficient strategies to optimise the power consumption of IoT devices. This includes intelligent sleep modes, dynamic power allocation, and energy-aware scheduling to prolong the lifespan of battery-operated devices and ensure continuous operation. DRF-IoT is designed to continuously learn and adapt to changing conditions, usage patterns, and environmental factors.

It leverages machine learning and A.I. algorithms to improve its decision-making processes and enhance the overall reliability of the IoT system over time. This conceptual framework's practical implementation would require detailed design, development, and validation. As technology evolves, additional improvements and enhancements may be integrated into the DRF-IoT to ensure it remains effective in improving the reliability of IoT systems.

This novel model for the reliability of Internet of Things associates the reliability frame, machine learning algorithms, security capabilities and their comparative performance evaluation based on transmission, perception, processing and system reliability, as depicted in Figure 3. This novel model improves the accuracy and precision of securing machine learning models on various Internet of Things datasets acknowledging the performance evaluation in designing techniques.

Recently, with the growth of IoT applications in many fields, the need for reliability has increased due to the negative effects that setbacks may have on the display of IoT frameworks. The effects might be terrible in rural areas. IoT system flaws might begin in the communication framework, energy framework, mechanical framework, and so on. Table 1 summarises the research on present problems with the Internet of Things dependability, suggested solutions and potential future developments. IoT frameworks continue to be composed of a few building blocks.

Table 1. Evaluation of work analysis and future prospective of different research articles in the detailed view of the reliability of the Internet of Things

Year	Author's name	Research title	Proposed work	Future scope
2023	J. Gong	"An application of meta-heuristic and nature-inspired algorithms for designing reliable networks based on the Internet of Things: A systematic literature review"	Reliable improvement strategies improve longevity and efficiency, including detecting failure nodes in IoT networks.	I learned from the literature that the present research concentrates on the requirements linked to employing edge network features for IoT application deployments enabling support for the future.
2022	Dong-Seong Kim, T. Hoa, Huynh-The Thien	"On the Reliability of Industrial Internet of Things from Systematic Perspectives: Evaluation Approaches, Challenges, and Open Issues"	The unavailability of standard foundations for Internet of Things systems with varied reliability levels presented numerous interesting options for the practical application of the study.	We anticipate focusing more on academics along with practitioners' efforts on creating solid frameworks as well as approaches.
2022	Alyzia Konsta, Alberto Lluch-Lafuente, N. Dragoni	"Trust Management for Internet of Things: A Systematic Literature Review"	By giving each node a trust value that indicates its degree of trust, trust management tries to assure the dependability of the entire network.	A categorisation based on the methodologies used in each study, a discussion of the unresolved problems, including future research prospects. Existing trust management strategies for IoT.
2021	Shiwei Xue	"Construction of reliability evaluation model of power Internet of Things based on Bayesian network"	Creating an energy-efficient Internet of Things framework that facilitates Bayesian network-based reliability assessment.	A few forthcoming study paths that are relevant for reliability experts are indicated, along with an examination of the current gaps as well as difficulties in reliability assessment using B.N.s.
2021	Mohammad Zubair Khan, O.H. Alhazmi, M. Javed	"Reliable Internet of Things: Challenges and Future Trends"	A key element of the future of enterprise is the Internet of Things.	IoT security based on blockchain, 6G connectivity, and dependable machine learning approaches needs more study and deliberation of associated future prospects.

2021	Franklin Magalhães Ribeiro Junior,Carlos Alberto Kamienski	"A Survey on Trustworthiness for the Internet of Things"	For devices based on mist and fog, the Reliability for IoT Framework provides data with a sense of reliability.	The TW-IoT In order to guarantee a continuous and continuous flow of Internet of Things data for future study, architecture offers data trustworthiness.
2021	S. M. Muzammal, R. Murugesan, N. Jhanjhi	"A Comprehensive Review on Secure Routing in the Internet of Things: Mitigation Methods and Trust-Based Approaches"	The trust models in IoT for secure routing are analysed.	The implications when it comes to trust measurements in IoT settings, routing protocols, open themes, and research challenges are addressed. Trust also functions as a security paradigm in IoT networks.
2020	Dong-Seong Kim	"Reliability Evaluation Model Of Industrial Internet of Things Systems"	A system's dependability is regarded as an indicator of efficiency that shows how precisely and correctly the system functions.	This approach makes it possible to clarify a number of unresolved research problems related to creating reliable as well as resilient systems.
2020	Yecheng Zhang, Guigen Zhou, N. Yang	"Research on the Reliability of Internet of Things Information Transmission for Bus Bar Operation Online Monitoring"	The approach and method put forth in this article can significantly lower the Internet of Things packet loss rate.	Effectively address the issue of the online monitoring system's information transfer dependability for bus bar operating status for the future.
2020	Li Xing	"Reliability in the Internet of Things: Current Status and Future Perspectives"	Research on the dependability of the Internet of Things is in its early stages.	Future elements of the evolving IoT infrastructure's growing complexity, dynamism, and difficult research issues and opportunities are underlined.
2020	Samuel J. Moore, Chris D. Nugent, Shuai Zhang, Ia	"IoT reliability: a review leading to 5 key research directions"	The ability to quantify the reliability of IoT devices, systems, and network is a critical function.	For quantifying dependability in the IoT, highlighting the many difficulties involved in this job. A number of important research objectives for IoT.
2020	Yi Lyu, Peng Yin	"Internet of Things transmission and network reliability in a complex environment"	The suggested technique enhances data fusion efficiency, transmission reliability, and overall network life cycle by reducing data transmission and energy usage.	Investigating the effect of a new communication connection on the mobile node's network capacity for future work and research.
2020	Yu-chang Mo, L. Xing, Wenzhong Guo, Shaobin Cai…	"Reliability Analysis of IoT Networks with Community Structures"	In comparison to the conventional ordering heuristics, the suggested ordering heuristics perform noticeably better in terms of model complexity.	The suggested ordering heuristics outperform the conventional ordering heuristics in terms of model complexity via extensive trials.
2020	Kazim Ergun, Xiaofan Yu, N. Nagesh, L. Cherkasov	"Simulating Reliability of IoT Networks with RelIoT"	The power, temperature, and reliability characteristics of actual networked IoT devices are faithfully captured by RelIoT.	Our framework shows that RelIoT successfully models the reliability, power, and overall temperature dynamics of actual networked IoT devices.
2020	Shasha Li, Tiejun Cui, Muhammad Alam	"Reliability analysis of the Internet of Things using Space Fault Network"	The effectiveness of IoTNT is investigated in connection to potential logical relationships between nodes.	New methodologies for IoT reliability analysis and SFN creation are provided by research.

2020	Kamal Azghiou, Manal El Mouhib, M. Koulali, Abdel	"An End-to-End Reliability Framework of the Internet of Things"	The suggested framework is flexible, expressive, and highly scalable.	The numerical investigation provides mission time intervals that describe an IoT system's behaviour from the perspective of its dependability.
2020	Mohammed Sati, Tareg Abulifa, Salem Sati	"Wireless Link Reliability in Cyber-Physical System with Internet of Things"	Hardware parameters for routing protocols are categorised as link quality measurements.	The numerical results show that routing effectiveness and overall link quality may be divided into three quality zones, each corresponding to a different packet delivery ratio. There are three distinct colours: black, grey, and white.
2020	O. O. Illiashenko, M. A. Kolisnyk, A. E. Strielkina, I. V	"Conception and Application of Dependable Internet of Things Based Systems"	The article outlines a number of technological and scientific hurdles that must be overcome before meaningful Internet of Things-based applications can be built and used.	The opportunities for future study might include a detailed examination of the models, techniques, and technologies created to guarantee the reliability of complex data and managerial systems for IoT.

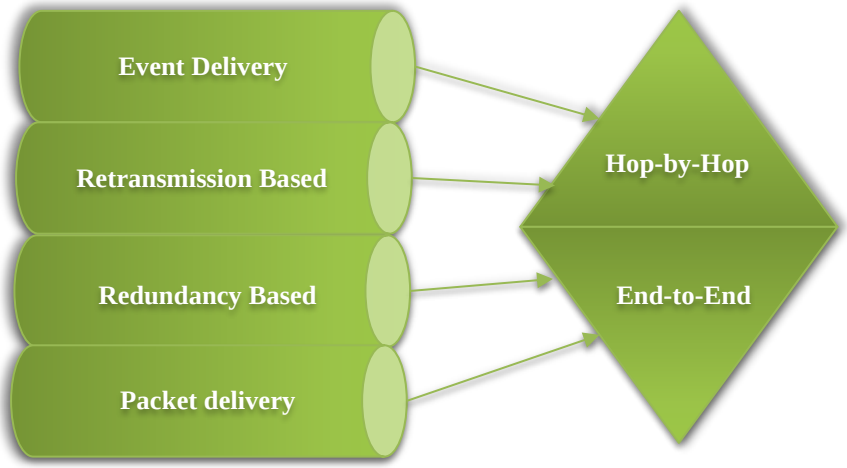

Fig. 4 Reference model for the WSN reliability study

Communication, computing, storage, services, and applications round out the list. Our focus has been on increasing the communication square's reliability. The phrase "unwavering quality" may describe features such as use strength, security problem protection, adaptability, self-design, long-term usability, or overall framework dependability [22–25].

Unwavering IoT framework quality is essential for the system's overall dependability. Failure in being able to transmit sensor data in a trustworthy and practical way to improve system consistency, such as parts enhancement technique, strong and imaginative planning, utilisation of misrepresented segments, and auxiliary excess, where the latter offers reliability through elective sequences. [26].

An object is a bright thing in an IoT system where data is acquired via sensor hubs. The kind of utilisations that will be carried out must include the finest determination of sensors conceivable. Additionally, the framework may combine data from other sensors, opening up the possibility of recovering the accuracy and consistency of the information [27].

Since many IoT entries use easy sensors, it is reasonable to include extra parts. It can increase information accuracy thanks to these tools and excellent directing practices. Additionally, a surplus in order to reestablish the trustworthiness of IoT frameworks, the devices, including communication lines, may be checked. Saving the raw data for further processing is essential after information collection. Right now, repetition may also be considered with the goal of developing a trustworthy design.

To do this, cloud workers and knowledge bases in haze structures may both operate in a haze-based design. Fog phones may temporarily store data during system disruptions

and transmit it to an independent cloud worker once connectivity has returned. Additionally, despite the restricted transitory capacity of the information base due to repetition, it is still feasible to progress connections since not every material has to be fully retained [28].

3. Redundancy-Based IoT Reliability Framework

Retransmission and excess are two techniques often used to improve WSN dependability. Mahmood et al. [8] provide a three-dimensional reference representation of WSN without compromise (Fig. 4). To evaluate the dependability as well as the efficiency of wireless sensor networks (WSNs), particularly in important uses where reliability is vital, a reliability study of WSNs is necessary. The study involves evaluating various factors that influence the reliability of WSNs and understanding their behaviour under different conditions. Here are key aspects to consider in a reliability study of wireless sensor networks:

3.1. Node Reliability Assessment and Reliability Communication

Evaluate the individual nodes' reliability in the WSN. This includes analysing factors such as hardware robustness, power supply stability, and temperature resilience. Understanding how individual nodes perform under stress is critical to overall network reliability. Assess the reliability of communication links between nodes. This involves measuring the packet loss rates, signal strength, and latency in transmitting data between nodes. Communication reliability is crucial as nodes collaborate to transfer data towards the sink or gateway.

3.2. Network Topology Resilience and Energy Efficiency

Study the network's resilience to topology changes due to node failures, mobility, or environmental conditions. Understanding how the network adapts and recovers from these changes is vital in maintaining reliable connectivity. Find out how the network as a whole and its individual nodes use energy. Assessing the network's energy efficiency and node battery life is important to guarantee long-term and dependable network operation.

3.3. Reliability Under Interference and Noise

Examine how WSNs perform under various types of interference, noise, or coexistence with other wireless networks. Robustness against interference ensures reliable data transmission and reception.

3.4. Redundancy and Fault Tolerance

Analyse the redundancy mechanisms and fault tolerance strategies implemented in the WSN. This includes evaluating how the network responds to node failures and how redundant nodes help maintain continuous data flow.

3.5. Reliability in Harsh Environments

Study the performance of WSNs in challenging or harsh environments, such as extreme temperatures, high humidity, or areas with limited access. Understanding how the network behaves in such conditions is crucial for mission-critical applications. Evaluate the network's security measures to ensure data integrity and confidentiality. A reliable WSN must protect against unauthorised access, data tampering, and malicious attacks.

3.6. Reliability in Mobility Scenarios

Investigate how the network performs when mobile nodes are deployed in dynamic environments. This includes understanding handover and routing mechanisms to maintain reliable connections. Conduct real-world deployment studies to validate the findings in practical scenarios and observe the network's reliability under real operational conditions. A comprehensive reliability study of wireless sensor networks helps identify potential weaknesses and areas for improvement, leading to more robust and dependable IoT applications and solutions. The study results can also guide network design, protocol selection, and optimisation strategies to enhance the overall reliability of wireless sensor networks[29-31].

4. Redundancy-Based Models for the IoT

Redundancy-based reliability models are crucial for continuous operation, including fault tolerance in the IoT setting. Redundancy involves using duplicate or backup components to maintain system functionality even in the presence of failures or errors. Here are some common IoT reliability models based on redundancy:

4.1. Active and Standby Redundancy

Active redundancy involves deploying multiple identical IoT devices or components that work simultaneously in an active state. If one device fails, the redundant device takes over immediately, ensuring continuous operation. This model is often used in critical applications where downtime is not acceptable. Standby redundancy consists of deploying N primary IoT devices along with one redundant backup device. The redundant device is in standby mode and remains inactive unless one of the primary devices fails. When a failure occurs, the backup device becomes active to replace the failed one.

4.2. Hot and Cold Standby Redundancy

Hot standby redundancy involves having two identical IoT devices operating in parallel, with one device actively processing data and the other on hot standby. The standby device continuously monitors the active device's health and takes over immediately if the active device fails. Cold standby redundancy is similar to hot standby redundancy, but the redundant device remains in a cold, powered-off state until needed. When the active device fails, the redundant device is powered on and takes over the operation.

4.3. Diverse and Triple Modular Redundancy (TMR)

Diverse redundancy involves using different types of IoT devices or components to provide redundancy. By using diverse technologies or architectures, the system can defend against common-mode failures and improve overall reliability. TMR is a particular kind of N-modular redundancy in which three identical components or devices operate in parallel. The proper output is decided via a voting system, and even if one of the devices fails, the other two may always outvote it to get an accurate result. TMR is often used in safety-critical systems.

4.4. Software and Communication Path Redundancy

In software redundancy, critical functions or processes are duplicated in the software, and if one instance fails, the redundant instance takes over. This can be achieved through code replication, voting mechanisms, or graceful degradation approaches. Communication path redundancy involves deploying multiple communication paths between IoT devices or nodes. If one path fails or becomes congested, data can be rerouted through an alternative path, ensuring continuous data transmission.

Each reliability model based on redundancy provides various levels of fault tolerance and dependability for IoT systems.

Considerations, including application importance, budget, and desired dependability, play a role in deciding which redundancy model is best for a given Internet of Things implementation.

Their excess restores general consistency due to how crucial variables continue functioning in IoT systems. It is feasible to create a straight, unwavering quality model in this manner equivalent to entering and counting severance. Each gateway here is connected to a standby gateway; as a result, the two form a master-slave pair.

This is seen in Figure 5. Figure 6 shows another alternative design in which just one redundant connection is considered for each primary connection from each gateway to the server. However, employing both correspondence joins and door repetition in this model, as illustrated in Fig. 7, improves consistency.

To acquire the extra connections, two specialised systems having connections to different ISPs or two independent system upgrades may be employed. The model in Fig. 7 may be changed to meet any scenario where devices coordinate for variables, something that's a common occurrence in daily life [33-35].

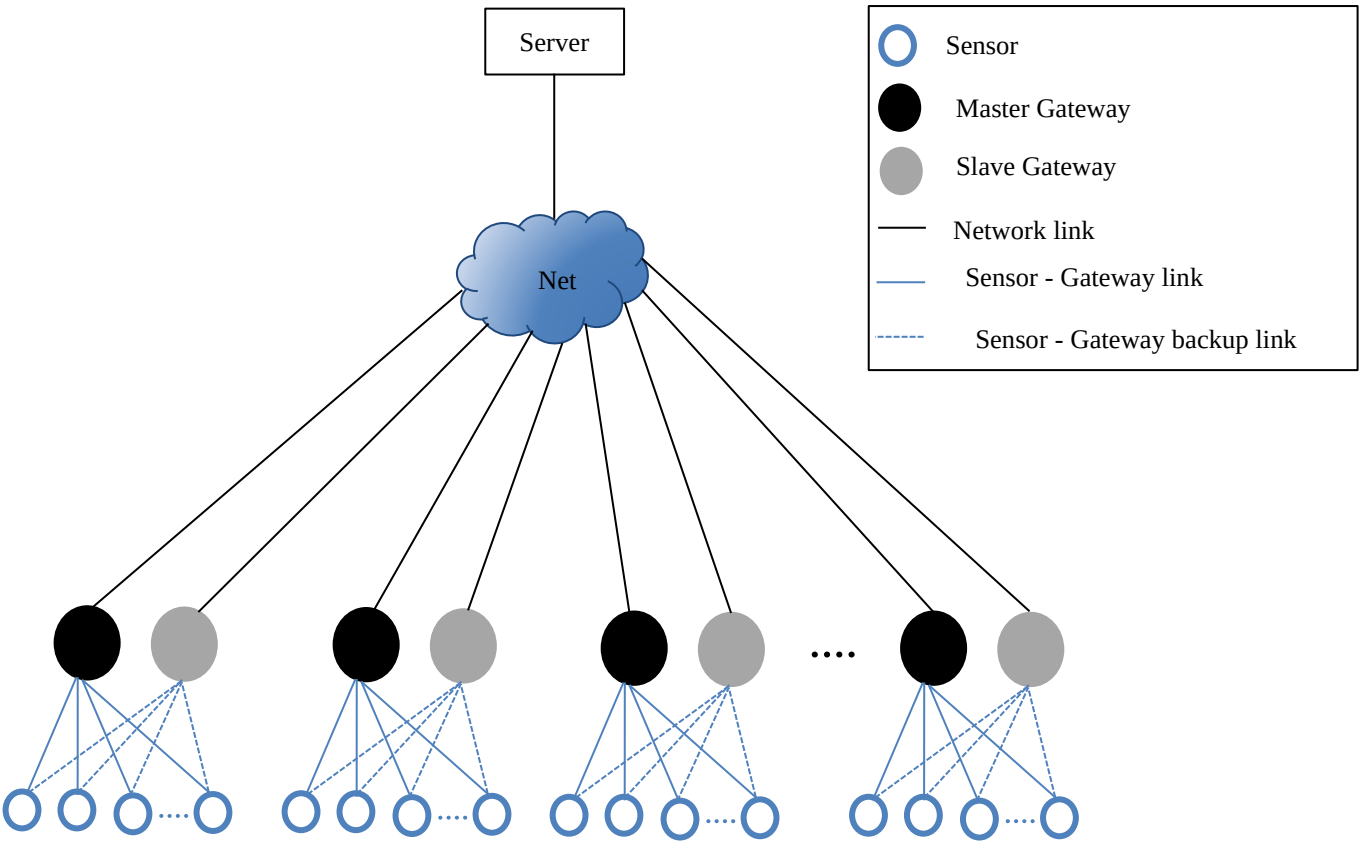

Fig. 5 Model for reliability through redundant gateways [56]

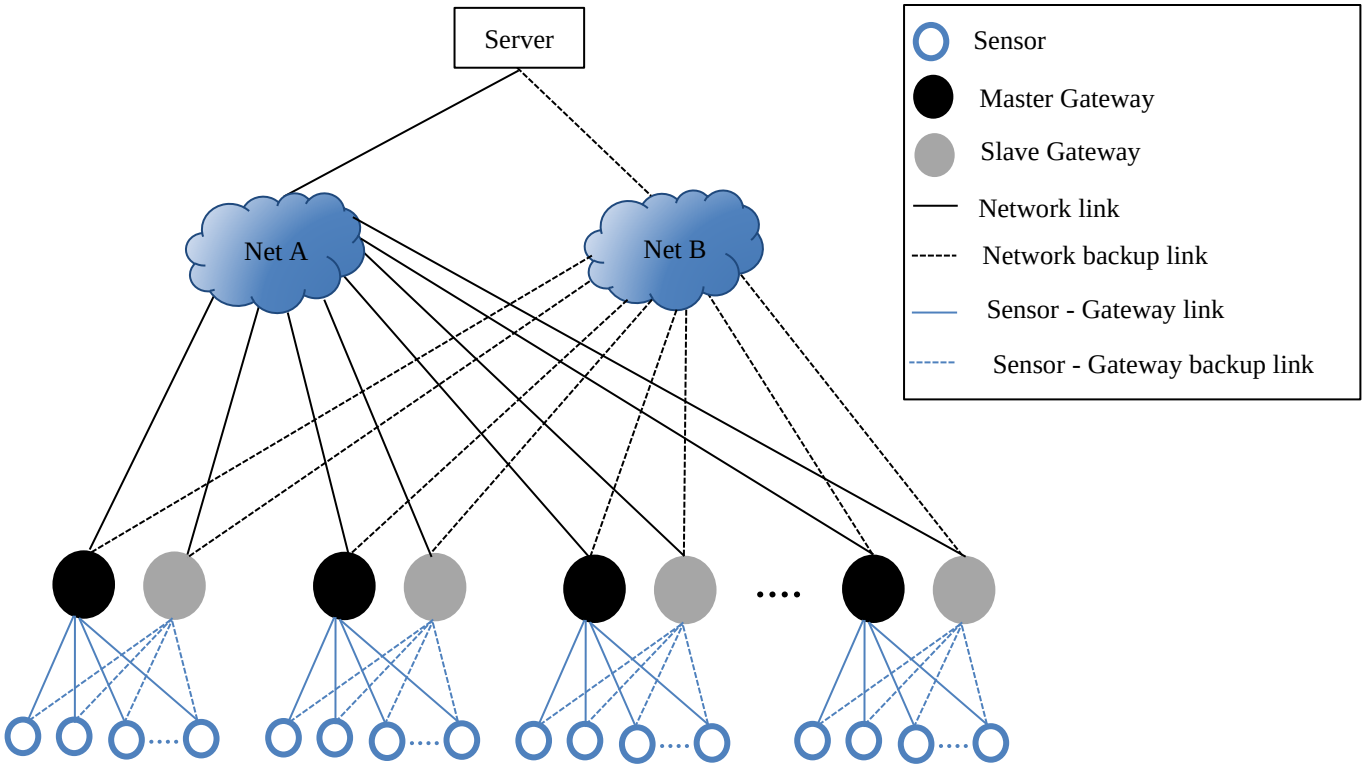

Fig. 6 Model of dependability using redundancy in communication [56]

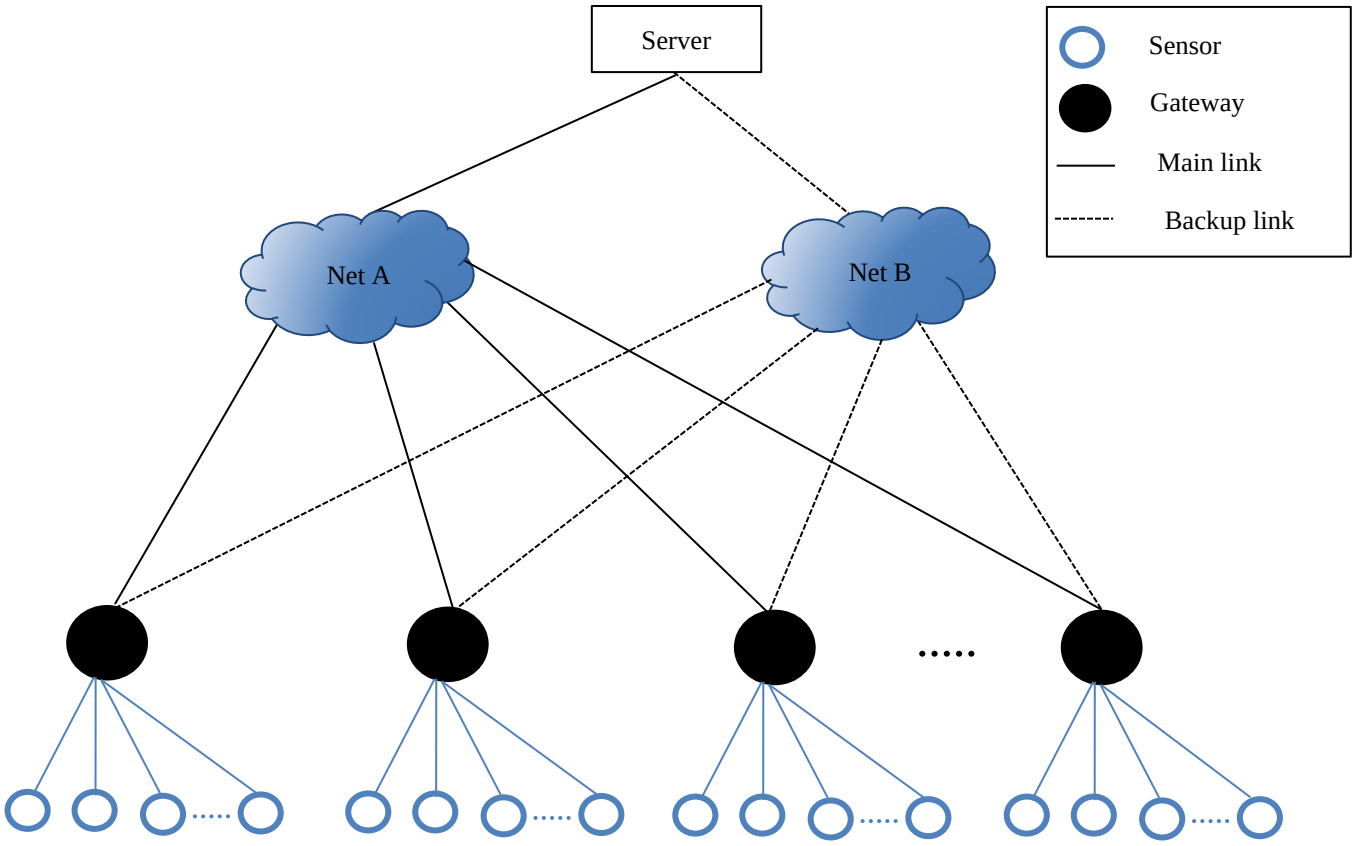

Fig. 7 Dual redundancy assessment of reliability within the IoT reliability paradigm [56]

5. Precise Demonstrating of IoT System Reliability

A framework is increasingly vulnerable to setbacks as it grows in size and complexity, which affects how it is shown [36]. IoT frameworks should address this problem as well. Using components and extra-way variation is one effective technique to achieve this. Demonstrating the reliability of an Internet of Things (IoT) system requires a systematic and thorough approach to showcase its dependability and robustness. It is possible to demonstrate the stability of frameworks using diagrammatic reasoning. The use of the diagram hypothesis for reliability considerations went according to plan. Utilising this kind of inquiry light has become more important nowadays because of the system [63].

Assessing dual redundancy in the IoT reliability model involves evaluating the effectiveness and dependability of redundant components or devices deployed in the system. Dual redundancy refers to having two identical components working in parallel, providing backup and fault tolerance to ensure continuous operation in case one component fails. "Non-state-space models In the context of IoT (Internet of Things), non-state-space models refer to mathematical or analytical models used to describe and analyse the behaviour of IoT systems without explicitly representing the state of the system. Unlike state-space models, which track the internal state variables of the system over time, non-state-space models focus on the input-output relationship and behaviour of the system without explicitly modelling its internal dynamics.

These non-state-space models offer flexible and efficient approaches to analysing and modelling the behaviour of IoT systems without explicitly tracking internal states. They provide valuable insights and predictive capabilities, making them essential tools in IoT applications across various domains [38]. A Reliability Block Diagram (RBD) is a graphical representation used to model and analyse the reliability of complex systems. It is a powerful tool commonly employed in engineering, including applications in the field of IoT (Internet of Things). The primary purpose of an RBD is to depict the structure of a system by breaking it down into individual components and representing their relationships in terms of reliability.

In an RBD, system components are represented as blocks, and the connections between them are shown as arrows or lines. The blocks represent various elements, such as devices, subsystems, or functional units, contributing to the overall system's performance. The arrows indicate the flow of reliability from one component to another. Inclusive, Engineers and analysts might benefit from a dependability block diagram because it visually depicts the system's reliability structure about system design, maintenance strategies, and fault tolerance measures to enhance the overall reliability of complex systems, including those found in IoT applications.

In the Internet of Things (IoT) context, a Fault Tree Analysis (FTA) is a systematic and graphical approach used to analyse and assess the potential causes of system failures or undesirable events. FTA is a powerful tool for evaluating the reliability and safety of IoT systems by identifying the various fault events and their potential combinations that could lead to system failures [39-42]. In this work, it has been tested the dependability of the proposed recurring models using previous formalisms, including Randomised Block Design and Unyielding Quality Charts/Systems. A basic RBD model collects dissatisfaction ratings [46] before module layout.

Three iterative scenarios have been analysed in line with the reliability models given in this section. The barebones IoT infrastructure has a worker, an ISP, a corridor, and an embedded sensor system; it has no unnecessary components and is built from prefabricated modules. Passage's Internet of Things architecture meets ISP coverage. To evaluate the dependability of an Internet of Things (IoT) system using appropriate models, the following three repeat scenarios can be considered, each aligned with different aspects of IoT dependability models:

5.1. Redundancy Evaluation Scenario

Assess the reliability and fault tolerance of the IoT system under redundancy mechanisms. This scenario aligns with redundancy-based dependability models, such as N-modular redundancy, dual redundancy, or hot standby redundancy. Evaluate how the IoT system performs when redundant components are introduced, and assess how the redundancy mechanisms contribute to improving fault tolerance and system reliability. Intentionally induce failures in individual components and observe how redundant components take over to maintain continuous operation. Calculate the system's reliability with and without redundancy to demonstrate the impact on overall dependability.

5.2. Data Integrity and Security Scenario

Analyse the dependability of data integrity and security measures in the IoT system. This scenario aligns with security-based dependability models, ensuring data confidentiality, integrity, and protection against cyber-attacks. Evaluate how the IoT system safeguards against data tampering, unauthorised access, and malicious attacks, ensuring that data remains accurate and secure. Attempt to breach the system's security measures, inject fake data, or perform unauthorised access. Assess how well the IoT system detects and mitigates these security threats and ensures data integrity.

5.3. Resource Management and Energy Efficiency Scenario

Assess the dependability of resource management and energy efficiency in the IoT system. This scenario aligns with

efficiency-based dependability models, ensuring optimal resource utilisation and prolonged device battery life. Evaluate how the IoT system manages resources efficiently, avoiding resource depletion and optimising energy consumption. Monitor and record resource usage under different operational scenarios, such as CPU, memory, and network bandwidth. Assess how well the system optimises resource allocation to ensure efficient performance and longer battery life in battery-powered IoT devices.

By incorporating these three repeat scenarios aligned with different aspects of IoT dependability models, you can comprehensively evaluate the system's robustness, security, and efficiency. The results of these evaluations will provide valuable insights for improving the overall dependability and reliability of the IoT system. One-way or two-way relationships and connections are also possible.

A Block Design Diagram (BDD) is a graphical representation that illustrates the high-level architecture and interactions of various components in an IoT system. It is a useful tool for visually depicting the relationships between different blocks or modules, helping stakeholders and developers understand the system's structure and functionalities. The Aggregate of Disjoint Items (SDP) and the Parallel Choice Charts are two of the several techniques for assessing the dependability articulation BDDs). Figure 8 depicts the reliability block diagram of the basic IoT System redundancy of the gateway.

An SDP is based upon the Boolean capacity personality; the Reduced Ordered Binary Decision Diagram (ROBDD) is not directly related to the typical applications of IoT systems. ROBDDs are primarily used in the fields of computer science and engineering for efficient representation and manipulation of Boolean functions, as mentioned in the previous response. However, in certain cases, ROBDDs might indirectly come into play when dealing with complex decision-making processes or logic in IoT systems.

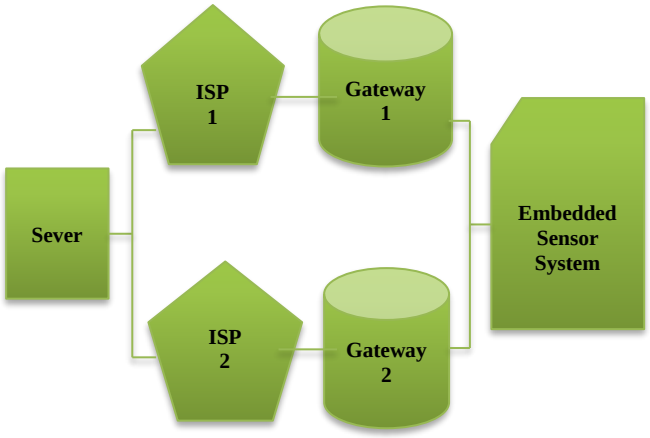

Fig. 8 Reliability for simple IoT system redundancy block diagram

5.3.1. Complex Rule-Based Systems

In some IoT applications, particularly in the domain of industrial automation and control, complex rule-based systems might be used for decision-making and control. ROBDDs could potentially be applied to represent and optimise these rule sets efficiently.

5.3.2. Verification and Model Checking

When formal verification techniques are used to ensure the correctness and reliability of IoT systems, ROBDDs could be employed in the model-checking process to analyse system properties and verify system behaviour.

5.3.3. System Optimisation

In IoT applications that involve complex logic expressions and decision paths, ROBDDs might be used to optimise the logic and reduce redundancy, leading to more efficient and streamlined operations.

While ROBDDs might not be directly applied in the typical IoT system development or data processing stages, they can still be valuable in certain specialised scenarios involving complex logic and rule-based decision-making [44-50].

In general, the primary focus in IoT development remains on designing efficient communication protocols, robust data handling, security, reliability, and energy efficiency rather than on using specific data structures like ROBDDs, factor-based parallel trees with a single level were utilised [51-55]. The pre-owned computation depends on the recursive implementation of the probabilistic interpretation of the Shannon degradation rule [56-62].

6. Conclusion

In this paper, Reliability Models with multiple links and alternative links are being analysed with their performances against the different studies with Reliabilities. A Novel model for the reliability of the Internet of Things is being proposed, which assesses the different reliability models through accuracy with different machine learning algorithms.

Finally, this paper examined the part of unwavering quality in systems devoted to article boards along with actual objects' "Internet of Things" perceptions. The Internet of Things seems distinct from the conventional internet in a number of important respects. A lot of applications are safety-critical, networks are often unmanaged, and the vast majority of nodes need to be implemented with little overhead.

The authors provide several architectural ideas for addressing dependability issues during packet transmission, during the lifetime of a network, as well as in the behavior of applications. It has been done by drawing on their experiences developing and implementing such networks.

References

[1] Houda Lhore et al., "Blockchain Technology as a Possible Solution to IoT Security Issues," *International Journal of Engineering Trends and Technology*, vol. 71, no. 1, pp. 152-163, 2023. [CrossRef] [Publisher Link]

[2] Kazim Ergun et al., "RelIoT: Reliability Simulator for IoT Networks," *Internet of Things-ICIOT 2020: 5th International Conference, Held as Part of the Services Conference Federation*, SCF 2020, Springer International Publishing, Honolulu, HI, USA, 2020, pp. 63-81, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Samuel J. Moore et al., "IoT Reliability: A Review Leading to 5 Key Research Directions," *CCF Transactions on Pervasive Computing and Interaction*, vol. 2, pp. 147-163, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Mohit Yadav, "A Review on Piezoelectric Energy Harvesting Systems based on Different Mechanical Structures," *International Journal of Enhanced Research in Science, Technology & Engineering*, vol. 9, no. 1, pp. 1-7, 2020. [Google Scholar] [Publisher Link]

[5] Marcantonio Catelani et al., "Reliability Analysis of Wireless Sensor Network for Smart Farming Applications," *Sensors*, vol. 21, no. 22, p. 7683, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Zhaoyi Xu, and Joseph Homer Saleh, "Machine Learning for Reliability Engineering and Safety Applications: Review of Current Status and Future Opportunities," *Reliability Engineering & System Safety*, vol. 211, p. 107530, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Liudong Xing et al., "Reliability Modeling of Mesh Storage Area Networks for Internet of Things," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2047-2057, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[8] Nourhene Maalel et al., "Reliability for Emergency Applications in Internet of Things," *IEEE International Conference on Distributed Computing in Sensor Systems*, Cambridge, MA, USA, pp. 361-366, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[9] Liudong Xing, "Reliability in Internet of Things: Current Status and Future Perspectives," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6704-6721, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Anand Singh Rajawat et al., "Reliability Analysis in Cyber-Physical System using Deep Learning for Smart Cities Industrial IoT Network Node," *AI and IoT for Smart City Applications*, pp. 157-169, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] M. Sandelic et al., "Reliability Aspects in Microgrid Design and Planning: Status and Power Electronics-Induced Challenges," *Renewable and Sustainable Energy Reviews*, vol. 159, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Xue-Qin Li, Lu-Kai Song, and Guang-Chen Bai, "Recent Advances in Reliability Analysis of Aeroengine Rotor System: A Review," *International Journal of Structural Integrity*, vol. 13, no. 1, pp. 1-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] S. Kholmirzayev et al., "Calculation of Reinforced Concrete Structures of Buildings Based on the Theory of Reliability," *Science and Innovation*, vol. 1, no. A8, pp. 1027-1032, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Heping Jia et al., "Reliability Evaluation of Demand-Based Warm Standby Systems with Capacity Storage," *Reliability Engineering & System Safety*, vol. 218, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Mohammed Hamouda Ali et al., "An Improved Wild Horse Optimization Algorithm for Reliability based Optimal DG Planning of Radial Distribution Networks," *Energy Reports*, vol. 8, pp. 582-604, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Mohit Yadav et al., "Modeling and Simulation of Piezo-beam Structure Mounted in a Circular Pipe using Laminar Flow as Energy Harvester," *International Journal of Engineering Trends and Technology*, vol. 71, no. 2, pp. 296-314, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Ming-Yang Su, "Real-Time Anomaly Detection Systems for Denial-of-Service Attacks by Weighted K-Nearest-Neighbor Classifiers," *Expert Systems with Applications*, vol. 38, no. 4, pp. 3492-3498, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[18] Gang Kou et al., "Reliability of a Distributed Data Storage System Considering the External Impacts," *IEEE Transactions on Reliability*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Adam Hulme et al., "Testing the Reliability and Validity of Risk Assessment Methods in Human Factors and Ergonomics," *Ergonomics*, vol. 65, no. 3, pp. 407-428, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Chunling Luo, Lijuan Shen, and Ancha Xu, "Modelling and Estimation of System Reliability under Dynamic Operating Environments and Lifetime Ordering Constraints," *Reliability Engineering & System Safety*, vol. 218, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[21] Wei-Chang Yeh et al., "Novel Binary Addition Tree Algorithm (BAT) for Calculating the Direct Lower-Bound of the Highly Reliable Binary-State Network Reliability," *Reliability Engineering & System Safety*, vol. 223, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Jari Metsämuuronen, "Attenuation-Corrected Estimators of Reliability," *Applied Psychological Measurement*, vol. 46, no. 8, pp. 720-737, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Herwin Herwin et al., "Do Scoring Techniques and Number of Choices Affect the Reliability of Multiple-Choice Tests in Elementary Schools," *Cypriot Journal of Educational Sciences*, vol. 17, no. 4, pp. 1258-1268, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Abebe Abeshu, and Naveen Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169-175, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[25] Nanda Kumar Thanigaivelan et al., "Distributed Internal Anomaly Detection System for Internet-of-Things," *13th IEEE Annual Consumer Communications & Networking Conference, IEEE,* pp. 319-320, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[26] Mohit Yadav et al., "State of Art of Different Kinds of Fluid Flow Interactions with Piezo for Energy Harvesting Considering Experimental, Simulations and Mathematical Modeling," *Journal of Mathematical and Computational Science*, vol. 11, no. 6, pp. 8258-8287, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[27] Ruoyu Zhang et al., "Integrated Sensing and Communication Waveform Design with Sparse Vector Coding: Low Sidelobes and Ultra Reliability," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4489-4494, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[28] Mohammad Najafzadeh, Farshad Homaei, and Sedigheh Mohamadi, "Reliability Evaluation of Groundwater Quality Index Using Data-Driven Models," *Environmental Science and Pollution Research*, vol. 29, no. 6, pp. 8174-8190, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[29] Mohit Yadav et al., "Experimental & Mathematical Modeling and Analysis of Piezoelectric Energy Harvesting with Dynamic Periodic Loading," *International Journal of Recent Technology and Engineering*, vol. 8, no. 3, pp. 6346-6350, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] Chayapol Kamyod, "End-to-End Reliability Analysis of an IoT Based Smart Agriculture," *International Conference on Digital Arts, Media and Technology, IEEE,* pp. 258-261, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[31] Mostafa Kazemi, and Mohammad Reza Ansari, "An Integrated Transmission Expansion Planning and Battery Storage Systems Placement-A Security and Reliability Perspective," *International Journal of Electrical Power & Energy Systems*, vol. 134, p. 107329, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[32] Georgios Spanos et al., "Combining Statistical and Machine Learning Techniques in IoT Anomaly Detection for Smart Homes," *IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, IEEE,* pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[33] Sajad Saraygord Afshari et al., "Machine Learning-Based Methods in Structural Reliability Analysis: A Review," *Reliability Engineering & System Safety*, vol. 219, p. 108223, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[34] Ashish Kaushik et al., "Advanced 3D Body Scanning Techniques and its Clinical Application," *International Conference on Computational Modeling, Simulation and Optimization, IEEE,* pp. 352-358, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[35] Aurora González-Vidal, Jesús Cuenca-Jara, and Antonio F. Skarmeta, "IoT for Water Management: Towards Intelligent Anomaly Detection," *IEEE 5th World Forum on Internet of Things, IEEE,* pp. 858-863, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[36] Mohit Yadav et al., "Modeling and Optimization of Piezoelectric Energy Harvesting System under Dynamic Loading," *Advances in Fluid and Thermal Engineering, Springer,* Singapore, pp. 339-353, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[37] I. Lakshmi, "Security Analysis in Internet of Things Using DDoS Mechanisms," *SSRG International Journal of Mobile Computing and Application*, vol. 6, no. 1, pp. 19-24, 2019. [CrossRef] [Publisher Link]

[38] Songyuan Li, and Jiwei Huang, "GSPN-based Reliability-Aware Performance Evaluation of IoT Services," *IEEE International Conference on Services Computing, IEEE,* pp. 483-486, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[39] Mannu Yadav et al., "Enhancing Dimensional Accuracy of Small Parts through Modelling and Parametric Optimization of the FDM 3D Printing Process using GA-ANN," *International Conference on Computational Modelling, Simulation and Optimization, IEEE,* pp. 89-94, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[40] Khushwant Singh, Dheerdhwaj Barak, and Yudhvir Singh, "Reviewing the IOT Systems Reliability and Accuracy," *The Pharma Innovation Journal*, vol. 12, no. 3, pp. 2775-2780, 2023. [Google Scholar] [Publisher Link]

[41] Sabrina Sicari et al., "A Security-and Quality-Aware System Architecture for Internet of Things," *Information Systems Frontiers*, vol. 18, pp. 665-677, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[42] Sabrina Sicari et al., "A Secure and Quality-Aware Prototypical Architecture for the Internet of Things," *Information Systems*, vol. 58, pp. 43-55, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[43] Himanshu Sawle, and Sandeep Parmar, "Restricted Area Security System based on IOT," *SSRG International Journal of Electronics and Communication Engineering*, vol. 5, no. 11, pp. 15-16, 2018. [CrossRef] [Publisher Link]

[44] Khushwant Singh, Dheerdhwaj Barak, and Yudhvir Singh, "IoT Chatbot in Insurance," *International Journal of Engineering, Management, Humanities and Social Sciences Paradigms*, vol. 33, no. 1, pp. 12-16, 2021. [Publisher Link]

[45] Mohit Yadav et al., "Piezo-Beam Structure in a Pipe with Turbulent Flow as Energy Harvester: Mathematical Modeling and Simulation," *Journal of the Institution of Engineers (India): Series D*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[46] Hitesh Kumar Sharma et al., "IoT Based Automatic Electric Appliances Controlling Device based on Visitor Counter," *International Journal of Psychosocial Rehabilitation*, vol. 10, no. 24, pp. 4186-4196, 2020. [Google Scholar] [Publisher Link]

[47] Mohit Yadav, and Dinesh Yadav, "Micro Energy Generation in Different Kinds of Water Flows on Lead Zirconium Titanate/PVDF," *International Journal of R & D in Engineering, Science and Management*, vol. 9, no. 5, pp.1-8. 2019. [CrossRef] [Google Scholar] [Publisher Link]

[48] Sven Nõmm, and Hayretdin Bahşi, "Unsupervised Anomaly based Botnet Detection in IoT Networks," *17th IEEE International Conference on Machine Learning and Applications, IEEE,* pp. 1048-1053, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[49] Mi Kim, "A Quality Model for Evaluating IoT Applications," *International Journal of Computer and Electrical Engineering,* vol. 8, no. 1, pp. 66, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[50] Bardia Safaei et al., "Reliability Side-Effects in Internet of Things Application Layer Protocols," *2nd International Conference on System Reliability and Safety, IEEE,* pp. 207-212, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[51] Yi Lyu, and Peng Yin, "Internet of Things Transmission and Network Reliability in Complex Environment," *Computer Communications*, vol. 150, pp. 757-763, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[52] Lixing Li et al., "Modeling and Analyzing the Reliability and Cost of Service Composition in the IoT: A Probabilistic Approach," *IEEE 19th International Conference on Web Services*, Honolulu, HI, USA, pp. 584-591, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[53] R. Raghu Nandan, and N. Nalini, "An Efficient Approach for Discovering Objects in the Internet of Things using Clue-Based Search Engine," *International Journal of Engineering Trends and Technology*, vol. 71, no. 3, pp. 282-294, 2023. [CrossRef] [Publisher Link]

[54] S. Karthikeyan, and T. Poongodi, "Secure and Optimized Communication in the Internet of Things using DNA Cryptography with X.509 Digital Attributes," *International Journal of Engineering Trends and Technology*, vol. 71, no. 3, pp. 1-8, 2023. [CrossRef] [Publisher Link]

[55] A. Kaleel Ahmed, C. B. Senthilkumar, and S. Nallusamy, "Study on Amalgamation of Internet of Things in Industrial Applications," *International Journal of Mechanical and Production Engineering Research and Development*, vol. 8, no. 1, pp. 1279-1286, 2018. [Google Scholar] [Publisher Link]

[56] Soraya Sinche et al., "Assessing Redundancy Models for IoT Reliability," *IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks,"* pp. 14-15, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[57] Akash Ahlawat et al., "Fabrication and Analysis of ABS-HDPE-PC Composite Polymer Filament Used for FDM Printing Using Hybrid Algorithm," *International Journal on Interactive Design and Manufacturing*, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[58] Krishna Yadav et al., "Effect of Speed, Acceleration, and Jerk on Surface Roughness of FDM-Fabricated Parts," *Journal of Materials Engineering and Performance*, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[59] Khushwant Singh et al., "Comparative Performance Analysis and Evaluation of Novel Techniques in Reliability for Internet of Things with RSM," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 9s, pp. 330-341, 2023. [Google Scholar] [Publisher Link]

[60] K. Singh et al., "Parametric Evaluation Techniques for Reliability of Internet of Things (Iot)," *International Journal of Computational Methods and Experimental Measurements*, vol. 41, no. 2, pp. 123-134, 2023. [CrossRef]

[61] Kiran Sood et al., "Identification of Asymmetric DDoS Attacks at Layer 7 with Idle Hyperlink," *ECS Transactions*, vol. 107, no. 1, p. 2171, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[62] Sandeep Bhatia et al., "A Comprehensive Review of IoT Reliability and its Measures: Perspective Analysis," *Handbook of Research on Machine Learning-Enabled IoT for Smart Applications across Industries*, pp. 365-384, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[63] Ashish Kaushik et al., "Optimization of Process Parameters for Scanning Human Face using Hand-Held Scanner," *Research Square,* 2022. [CrossRef] [Google Scholar] [Publisher Link]