Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 256 (2025) 55–62

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2024

Techniques in reliability of internet of things (IoT)

Khushwant Singh[a], Mohit Yadav[b], Yudhvir Singh[c], Fernando Moreira[d,*]

[a,c]*Department of Computer Science & Engineering,U.I.E.T, Maharshi Dayanand University Rohtak-124001,India*
[b]*Department of Mathematics, University Institute of Sciences, Chandigarh University, Mohali-140413,Punjab,India*
[d]*REMIT, IJP, Universidade Portucalense, Porto & IEETA, Universidade de Aveiro, Aveiro, Portugal*

Abstract

The Internet of Things (IoT) has rapidly transformed the way we interact with technology, connecting numerous smart devices to the internet. However, with the proliferation of IoT applications, ensuring the reliability of these interconnected systems has become a critical concern. The current paper presents the reliability of IoT systems achieved through a combination of fault tolerance, robust communication protocols, data integrity, predictive maintenance, energy efficiency, and comprehensive testing. By adopting these techniques, IoT deployments can ensure dependable and resilient operations, fostering the growth and adoption of IoT technologies across diverse industries. This abstract highlights various techniques employed to enhance the reliability of IoT systems. Fault tolerance plays a crucial role in increasing IoT system reliability. Redundancy techniques such as replication and backup are applied to ensure continued functionality in the event of device failures. Additionally, fault detection and self-healing mechanisms are integrated into IoT devices, allowing them to identify and correct errors autonomously. Robust communication protocols are essential to maintain reliable connections among IoT devices. These protocols should be designed to handle intermittent network connectivity, reduce latency, and ensure secure data transmission. Solutions like message queuing telemetry transport (MQTT) and Constrained Application Protocol (CoAP) are commonly used for their lightweight and efficient communication properties. Data integrity and security are paramount in IoT applications. Various cryptographic techniques, like asymmetric encryption and digital signatures, are implemented to safeguard data and prevent unauthorized access. Moreover, regular security audits and updates are necessary to address emerging threats and vulnerabilities. Predictive maintenance is a valuable technique for enhancing IoT device reliability. By utilizing sensors and analytics, IoT systems can monitor the status of all linked devices in real-time, allowing for preventative maintenance to be performed before any malfunctions develop. Battery-operated Internet of Things devices benefit greatly from energy-efficient design. Strategies for reducing energy consumption and maximizing performance include using low-power hardware design, optimizing data transfer, and entering a sleep state. Rigorous

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: fmoreira@upt.pt

Peer-review under responsibility of the scientific committee of the CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies
10.1016/j.procs.2025.02.095

testing and simulation environments are essential for assessing IoT system reliability. Robust testing helps identify and rectify potential issues before deployment, reducing the risk of system failures in real-world scenarios in the IoT system which increases the efficiency and reliability of IoT designs and Networks.

Peer-review under responsibility of the scientific committee of the CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies

Keywords: Reliability; Internet of things; Network reliability; Fault tree; CHISS

1. Introduction

Ensuring the reliability of Internet of Things (IoT) systems is crucial for their successful deployment and operation. IoT devices and networks often involve complex interactions and dependencies, making reliability a challenging but essential aspect to address [1-3]. Key components of an IoT system are such as device sensors, data processing, Applications and Services, and Security and Privacy [4-6]. These are the physical objects or devices equipped with sensors, such as temperature sensors, motion detectors, or GPS trackers, that collect data from the environment. IoT devices rely on various communication technologies to connect and transmit data [7-8]. This can include Wi-Fi, Bluetooth, cellular networks, or specialized IoT protocols like Zigbee or LoRaWAN. The collected data from IoT devices is sent to cloud-based or edge computing platforms, where it is processed, analyzed, and stored. This data processing enables real-time monitoring, insights, and decision-making. IoT data can be utilized by applications and services to provide specific functionalities or benefits [9-11]. For example, home automation systems can use IoT data to control lighting, temperature, and security systems. Industrial IoT can optimize manufacturing processes and predictive maintenance [12-14]. The sheer volume of interconnected devices and the associated risks make security a top priority in the IoT. Protecting IoT systems and user data requires the use of tools like encryption, authentication, and access control. Potential advantages of the IoT include better productivity, safer environments, and more convenient living [15-17]. Concerns regarding privacy, security, and the possible exploitation of personal data are also raised by this. These issues must be resolved, and adequate protections put in place to protect users and their data as the Internet of Things (IoT) develops further [18-20]. Figure 1 depicts the predicted global user population of connected IoT devices in the year 2025.

.

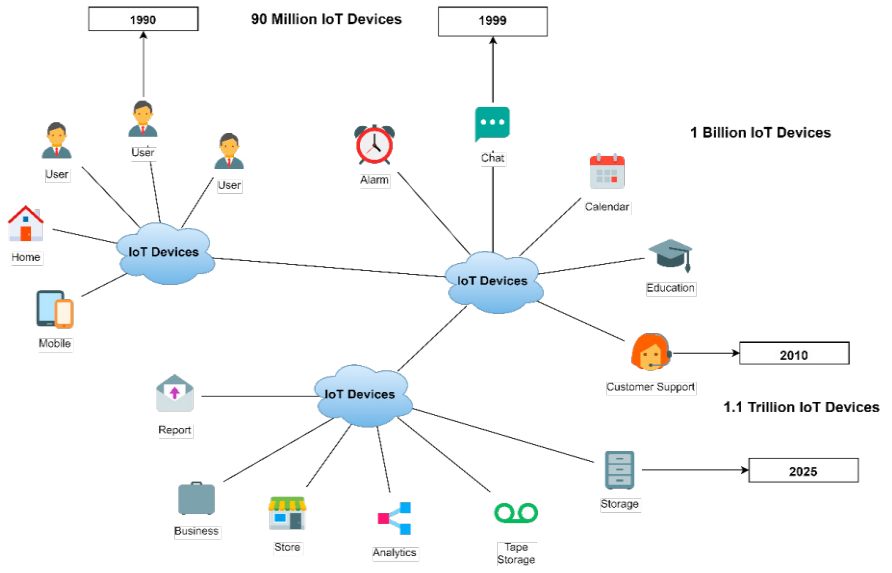

Fig.1. Number of IoT devices by 2025

Achieving reliability in IoT systems involves several key strategies. Fault tolerance is crucial, incorporating redundancy and failover mechanisms to maintain operation during component failures. Robust communication protocols, such as MQTT and CoAP, ensure stable and secure data transmission even under adverse conditions. Ensuring data integrity through encryption, checksums, and digital signatures protects against data corruption and unauthorized access. Predictive maintenance uses data analytics and machine learning to foresee and prevent equipment failures, minimizing downtime. Optimizing power consumption with efficient hardware design and low-power protocols enhances energy efficiency, prolonging device battery life. Comprehensive testing, including functional, performance, security, and stress testing, helps identify and mitigate potential issues before deployment, ensuring the system's long-term reliability and robustness. The sensing process depends on the interconnectedness of the modules. The term “Internet of Things (IoT)” refers to a network of actual physical goods, such as machines, vehicles, appliances, and other things, that are outfitted with sensors, software, and networking capabilities to collect and exchange data via the internet [21-23]. The success of implementing and running IoT systems depends heavily on their dependability [24-26]. However, due to the complex and dynamic nature of IoT systems, assessing their dependability presents new issues. Reliable assessment and quantification tools for Internet of Things (IoT) systems are lacking. The investigation of system characteristics and their effect on dependability is the focus of parametric assessment methods. Therefore, the stated objective is to create and standardize parametric assessment methods that accurately capture and measure IoT system dependability. It illustrates the difficulties inherent in designing and implementing an IoT system's dependability structure. IoT characteristics are discussed in Figure 2.

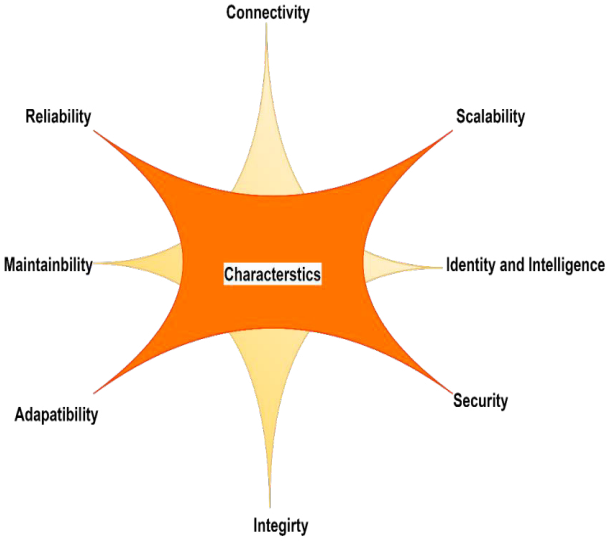

Fig.2 Characteristics of the internet of things

Designing an Internet of Things (IoT) system involves several key considerations to ensure its effectiveness, reliability, and security. Some important factors to consider when designing an IoT system include defining the use case, selecting the appropriate hardware, communication protocols, data collection and analytics, security and privacy, scalability and interoperability, user experience, power management, testing and validation, and regulatory compliance. It must define the purpose and objectives of your IoT system. Identification of the specific problem is the need of hours to aims the desired outcomes [27-29]. This will guarantee that the system achieves its intended goals and serve as a guide for the entire design process Depending on the specifications of the device's scenario, select the proper hardware and sensors. Consider factors such as power consumption, connectivity options, processing capabilities, and environmental considerations [30-33]. Make sure the communication protocols that intend to use and the hardware are compatible . Determine the most suitable communication protocols for your IoT system. Protocols such as Wi-Fi, Bluetooth, Zigbee, Z-Wave, or cellular networks can be selected based on the use case and device requirements. Consider factors such as range, bandwidth, power consumption, and data security.

2. Applications of the internet of things

The widespread adoption of Internet of Things (IoT) applications has significantly impacted various aspects of widespread adoption of Internet of Things (IoT) applications has significantly impacted various aspects of our lives, leading to increased efficiency, convenience, and connectivity. IoT has proven to be a transformative technology across industries, empowering businesses, governments, and individuals with valuable insights and data-driven decision-making capabilities. Smart Home, Smart Light, Smart Freeze, Smart CCTV, Smart Lock, Smart City, Smart Building, Smart Traffic, Urban Computing, Enhanced Security, Smart Health Care, Smart Wearable Patient Mentoring, Remote Health Monitoring, Smart Health Device, Smart Power Grid, Smart Solar, Smart Turbine, Smart Meter, Smart Industry etc. are various latest applications of Internet of things given in figure 3. Both MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) play vital roles in enhancing the reliability of Internet of Things (IoT) applications [34-36]. They are communication protocols specifically designed to address the unique challenges posed by resource-constrained IoT devices, ensuring efficient and dependable data exchange in IoT environments. Implementing cryptographic techniques like asymmetric encryption and digital signatures is essential in the IoT context to safeguard data, ensure confidentiality during transmission, verify data integrity, authenticate participants, and prevent unauthorized access or tampering. This

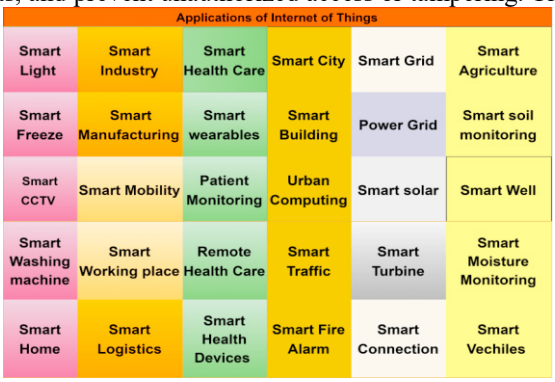

Fig. 3 Applications of Internet of Things

Security measures are integral to building trust in IoT systems and protecting sensitive information in a connected and potentially vulnerable environment. Figure 4 depicts the IoT support, application, communication, and perception reliabilities. Various real life examples such as fault tolerance, robust communication, data integrity, predictive maintenance, energy efficiency, and comprehensive testing enhances the reliability and performance of IoT systems in various industries

Fig.4 IoT support, application, communication, and perception reliabilities.

Reliability is defined as the probability i.e. a system performs its required function satisfactorily for a given period ‘t’ under the starting operating conditions. Reliability refers to the consistency and dependability of a measurement, assessment, or process in producing accurate and consistent results over time. High reliability is crucial in obtaining accurate and valid results, as it helps minimize errors and inconsistencies that could otherwise lead to misleading conclusions or unreliable predictions [37-38]. Researchers, engineers, and professionals in different fields strive to ensure and report high levels of reliability in their work to build confidence in the outcomes and their applications. In engineering, reliability refers to the consistency and dependability of a system, component, or process to perform its intended function without failure, within specified parameters, and over a defined period.

3. Reliability engineering

The goal of reliability engineering is to guarantee that a system or device will continue to work as designed even after being subjected to rigorous use for a long period. All phases of a system's creation, testing, manufacturing, and operation fall within the purview of reliability engineering. Several factors may be used to define reliability. The belief that something is suitable for a given purpose at a given time; The ability of a device or system to be executed as outlined; The resistance of a device or system to failure; The ability of a device or system to perform a required capacity under-expressed conditions for a given time frame. Statistics, probability theory, and reliability theory are all tools that are crucial to reliability engineers. To outline the reliability activities that will be done for a given system, most projects create a reliability programmed plan. This is due to the high cost of reliability approaches as well as the fact that various conditions call for different levels of dependability. Reliability engineering's purpose is to guarantee that a product will live up to its reliability specifications by formulating those specifications, creating a comprehensive reliability program, and carrying out all the necessary studies and activities. A reliability engineer oversees these duties, and they often have a formal engineering background in addition to reliability-specific training. Maintainability engineering and logistics engineering are subfields of reliability engineering. Reliability engineering methods may be used in many non-engineering situations. One example is security engineering. Varieties of Reliability Models for Systems can be concisely explained. The job of the engineer is to make educated guesses about the system's numerous reliability characteristics. The complexity of the system is not fixed. By breaking the system down into its parts and calculating the dependability of each, the overall system's reliability may be evaluated. Here is the process that must be followed to ascertain the dependability of the system. Determine what makes up the given system and its constituent parts.

Determine the individual dependability of the components and subsystems. Create a block diagram to show the interconnections between the various parts. Identifying the requirements for the system to function as intended. Determine the system's trustworthiness by using probability theory. System reliability is also the process of assigning probabilistic rules to the configuration of the system's components to establish a suitable dependability or reliability model for each component. Using high safety factors, simplifying the system, boosting the dependability of its components, and so on are only some of the ways to boost reliability. There are several setup options, including a series system, parallel system, and mixed system. In a series system, each part is linked directly to the next; this ensures that each part will have the power and current it needs to do its job. According to this theory, the whole system will crash if even a single serially linked part stops working. The components of a series system are linked in such a manner that the system will function properly only if every one of those components is functioning properly. The reliabilities of the individual parts make up the system's overall dependability.

4. Reliability in the internet of things

The reliability of IoT defines the transmission reliability in which end-to-end reliability, throughput, delay is to be defined, and moreover, software reliability assures edge computing, security, redundancy, and integrity. In Processing reliability, MTTR, MTTR, Fault tolerance, and protection performance metrics are to be used. Reliable packet transmission and delivery, as well as low power consumption, are crucial to the viability of an Internet of Things application. Information acquired and processed in real-time is essential in the Internet of Things, where sensors work together to monitor their surrounding environment. The reliability of an Internet of Things application relies heavily

on the consistency of its data transmissions. An IoT application's dependability is essential to its effective functioning; this is represented in the application's energy efficiency and prompt packet transfer. Real-time acquisition and prompt information processing are required on the Internet of Things, where sensors work together to perceive, gather, and analyze data in a monitoring environment. An important factor in determining the dependability of an IoT application is data transfer reliability. The reliability of energy efficiency in IoT is, however, only partially understood. This research study was able to develop knowledge of the mechanisms that support energy efficiency reliability in IoT. IoT device proliferation might result in a significant rise in the volume of data that is sent over the communication network. Thus, it would adversely affect the dependability of the application to reduce the energy requirements of these devices through an effective and reliable transmission network while processing data from the sensor devices as quickly as possible [38]. The Internet of Things (IoT) has become an increasingly important area of research in recent years, as it has the potential to revolutionize the way we interact with technology. However, one of the key concerns that researchers have focused on is the reliability of IoT systems. In this literature review, we will explore the current state of research on the reliability of IoT as depicted in figure 5.

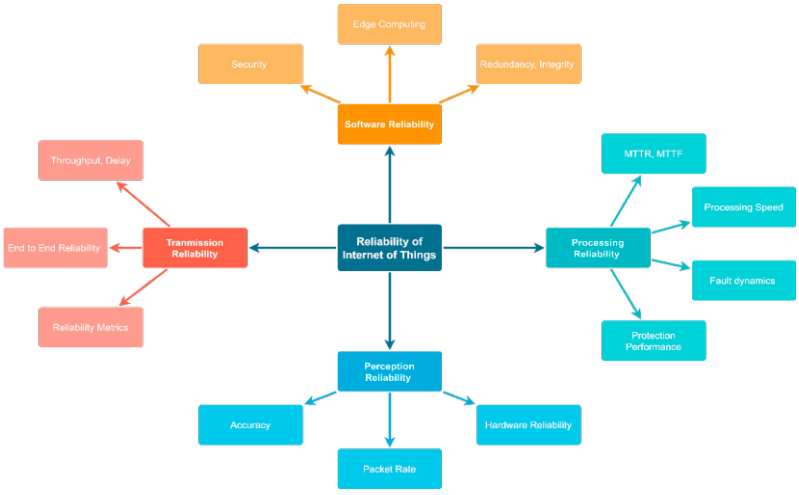

Fig.5 Reliability of Internet of Things

5. Overview of reliability in IoT with process parameters

IoT reliability refers to the ability of an IoT system to function as expected without any interruptions or failures. This is particularly important in mission-critical applications such as healthcare, transportation, and energy management. Reliable IoT systems require a robust and fault-tolerant architecture, which can cope with failures in individual components or nodes. Reliability of IoT process parameters refers to the robustness and dependability of various factors involved in the operation and functioning of an IoT system. Here are some important aspects related to the reliability of IoT process parameters such as hardware reliability, software reliability, data reliability, communication reliability, power management, security and privacy, fault detection and recovery, scalability, and resilience. The reliability of IoT devices and sensors is crucial for the overall performance of an IoT system. This includes the quality, durability, and failure rates of the hardware components used in IoT devices. Ensuring high-quality hardware with low failure rates helps maintain the reliability of the IoT system. The reliability of IoT software components, including firmware, operating systems, and applications, is essential. It involves ensuring that software is developed using best practices, follows rigorous testing and validation processes, and is resistant to vulnerabilities or bugs that could lead to failures or security breaches. Reliable data is a cornerstone of IoT systems. It involves data accuracy, consistency, and integrity throughout the data lifecycle, including data collection, transmission, storage, and analysis. Implementing data validation, error-checking mechanisms, and data redundancy strategies helps maintain data reliability in IoT systems. IoT systems rely on communication networks to transmit data between devices, gateways, and backend systems. Ensuring the reliability of communication channels, such as wired or wireless

networks, is crucial. This involves minimizing packet loss, latency, and ensuring network availability to maintain reliable and uninterrupted communication. Efficient power management is essential for IoT devices, especially those operating on limited power sources like batteries.

6. Conclusion

This paper presents how the reliability of IoT systems is achieved through a combination of fault tolerance, robust communication protocols, data integrity, predictive maintenance, energy efficiency, and comprehensive testing. By adopting these techniques, IoT deployments can ensure dependable and resilient operations, fostering the growth and adoption of IoT technologies across diverse industries. The augmentation and designing approach for improving the reliability of the Internet of Things (IoT) does offer significant benefits, but it also comes with certain limitations and challenges. Some of the key limitations include such as increased complexity, resource constraints, compatibility issues, heterogeneity, and interoperability. Implementing redundancy, fault tolerance, and other reliability-enhancing measures can add complexity to the IoT system. Managing and maintaining such complex systems may require specialized expertise and could lead to increased development and operational costs. Many IoT devices are resource-constrained, with limited processing power, memory, and battery capacity. Implementing certain reliability measures, such as encryption or advanced security protocols, might be resource-intensive and could affect device performance and battery life. Integrating diverse IoT devices from different manufacturers can lead to compatibility challenges, especially when adhering to multiple standards and protocols. This may hamper the seamless interoperability required for a reliable IoT ecosystem. Improved reliability prediction, anomaly detection, optimized maintenance strategies, data-driven decision-making, and energy efficiency are among the key areas where machine learning brings significant value. By leveraging the potential of machine learning, the research work contributes to the advancement and widespread adoption of reliable and efficient IoT technologies in various industries and domains in the future.

Acknowledgments

This work was supported by the FCT – Fundação para a Ciência e a Tecnologia, I.P. [Project UIDB/05105/2020]

References

[1] Moore SJ, Nugent CD, Zhang S, Cleland I. IoT reliability: a review leading to 5 key research directions.CCF Transactions on Pervasive Computing and Interaction. 2020 Oct ; **2**: 147-63. https://doi.org/10.1007/s42486-020-00037-z

[2] Singh K, Singh Y, Barak D, Yadav M. Evaluation of Designing Techniques for Reliability of Internet of Things (IoT). International Journal of Engineering Trends and Technology. 2023; **71(8)**:102-18. https://doi.org/10.14445/22315381/IJETT-V71I8P209

[3] Catelani M, Ciani L, Bartolini A, Del Rio C, Guidi G, Patrizi G. Reliability analysis of wireless sensor network for smart farming applications. *Sensors*. 2021 Nov 18; **21(22)**:7683. https://doi.org/10.3390/s21227683

[4] Xu Z, Saleh JH. Machine learning for reliability engineering and safety applications: Review of current status and future opportunities. *Reliability Engineering & System Safety* 2021 Jul 1; 211:107530.

[5] Xing L, Tannous M, Vokkarane VM, Wang H, Guo J. Reliability modeling of mesh storage area networks for Internet of Things. *IEEE Internet of Things Journal*. 2017 Sep 6; **4(6)**:2047-57. https://doi.org/10.1109/JIOT.2017.2749375

[6] Maalel N, Natalizio E, Bouabdallah A, Roux P, Kellil M. Reliability for emergency applications in internet of things. In 2013 IEEE international conference on distributed computing in sensor systems, 2013 May 20 (pp. 361-366). IEEE. doi: 10.1109/DCOSS.2013.40

[7] Xing L. Reliability in Internet of Things: Current status and future perspectives. *IEEE Internet of Things Journal*. 2020 May 7; **7(8)**:6704-21.

[8] Rajawat AS, Bedi P, Goyal SB, Shaw RN, Ghosh A. Reliability analysis in cyber-physical system using deep learning for smart cities industrial IoT network node. AI and IoT for Smart City Applications. 2022:157-69. https://rb.gy/kqws

[9] Sandelic M, Peyghami S, Sangwongwanich A, Blaabjerg F. Reliability aspects in microgrid design and planning: Status and power electronics-induced challenges.*Renewable and Sustainable Energy Reviews*. 2022 May 1;**159**:112127.

[10] Li XQ, Song LK, Bai GC. Recent advances in reliability analysis of aeroengine rotor system: a review. *International Journal of Structural Integrity*. 2022 Jan 12: **13(1)**:1-29. DOI 10.1108/IJSI-10-2021-0111

[11] Kholmirzayev S, Akhmedov I, Khamidov A, Akhmedov A, Dedakhanov F, Muydinova N. Calculation of reinforced concrete structures of buildings based on the theory of reliability. *Science and innovation* 2022; **1(A8):**1027-32. https://doi.org/10.5281/zenodo.7447650

[12] Jia H, Peng R, Yang L, Wu T, Liu D, Li Y. Reliability evaluation of demand-based warm standby systems with capacity storage. *Reliability Engineering & System Safety*. 2022 Feb 1; **218**:108132. https://doi.org/10.1016/j.ress.2021.108132

[13] Ali MH, Kamel S, Hassan MH, Tostado-Véliz M, Zawbaa HM. An improved wild horse optimization algorithm for reliability based optimal DG planning of radial distribution networks. *Energy Reports*. 2022 Nov 1; **8**:582-604. https://doi.org/10.1016/j.egyr.2021.12.023

[14] Singh K, Singh Y, Khang A, Barak D, Yadav M. Internet of Things (IoT)-Based Technologies for Reliability Evaluation with Artificial Intelligence (AI). InAI and IoT Tech. and Applications for Smart Healthcare Systems 2024 May 15 (pp. 387-395). Auerbach Publications.

[15 Hulme A, Stanton NA, Walker GH, Waterson P, Salmon PM. Testing the reliability and validity of risk assessment methods in Human Factors and Ergonomics. Ergonomics. 2022 Mar 4; **65(3)**:407-28. https://doi.org/10.1080/00140139.2021.1962969.

[16] Luo C, Shen L, Xu A. Modelling and estimation of system reliability under dynamic operating environments and lifetime ordering constraints. *Reliability Engineering & System Safety*. 2022 Feb 1; 218: 108136. https://doi.org/10.1016/j.ress.2021.108136

[17] Singh K, Singh Y, Barak D, Yadav M, Özen E. Parametric evaluation techniques for reliability of Internet of Things (IoT). *International Journal of Computational Methods and Experimental Measurements*. 2023:**11(2)**. https://doi.org/10.18280/ijcmem.110207

[18] Bhatia S, Goel N, Ahlawat V, Naib BB, Singh K. A Comprehensive Review of IoT Reliability and Its Measures: Perspective Analysis. Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries. 2023:365-84.

[19] Singh K, Singh Y, Barak D, Yadav M. Detection of Lung Cancers From CT Images Using a Deep CNN Architecture in Layers Through ML. InAI and IoT-Based Technologies for Precision Medicine 2023 (pp. 97-107). IGI Global.

[20] Singh K, Barak D, Singh Y. IoT Chatbot in Insurance. *International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS)*. 2021; **33(1)**:12-6.

[21] Abeshu A, Chilamkurti N. Deep learning: The frontier for distributed attack detection in fog-to-things computing. *IEEE Communications Magazine*.2018 Feb 13; **56(2)**:169-75. https://doi.org/10.1109/MCOM.2018.1700332

[22] Singh K, Barak D. Healthcare Performance in Predicting Type 2 Diabetes Using Machine Learning Algorithms. InDriving Smart Medical Diagnosis Through AI-Powered Technologies and Applications 2024 (pp. 130-141). IGI Global.

[23] Sood K, Dev M, Singh K, Singh Y, Barak D. Identification of Asymmetric DDoS Attacks at Layer 7 with Idle Hyperlink. ECS Transactions. 2022 Apr 24;**107(1)** :2171. DOI 10.1149/10701.2171ecst

[24] Singh K, Singh Y, Barak D, Yadav M. 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*. 2023 Jul 11; **11(9s)**:330-41. https://ijisae.org/index.php/IJISAE/article/view/3123

[25] Spanos G, Giannoutakis KM, Votis K, Tzovaras D. Combining statistical and machine learning techniques in IoT anomaly detection for smart homes. In2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) 2019 Sep 11 (pp. 1-6). IEEE. https://doi.org/10.1016/j.ress.2021.108223

[26] Afshari SS, Enayatollahi F, Xu X, Liang X. Machine learning-based methods in structural reliability analysis: A review. *Reliability Engineering & System Safety*. 2022 Mar 1;219:108223. https://doi.org/10.1016/j.ress.2021.108223

[27] Yadav M, Kumar S, Kaushik A, Chhabra D. 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*. 2023 Dec; **104(2)**:739-52.

[28] Bhatia S, Goel AK, Naib BB, Singh K, Yadav M, Saini A. Diabetes Prediction using Machine Learning. In2023 World Conference on Communication & Computing (WCONF) 2023 Jul 14 (pp. 1-6). IEEE. https://doi.org/10.1109/WCONF58270.2023.10235187

[29] Yadav M, Kaushik A, Garg RK, Yadav M, Chhabra D, Rohilla S, Sharma H. Enhancing dimensional accuracy of small parts through modelling and parametric optimization of the FDM 3D printing process using GA-ANN. In2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO) 2022 Dec 23 (pp. 89-94). IEEE. https://doi.org/10.1109/ICCMSO58359.2022.00030

[30] Li S, Huang J. GSPN-based reliability-aware performance evaluation of IoT services. In 2017 IEEE International Conference on Services Computing (SCC) 2017 Jun 25(pp. 483-486). IEEE. https://doi.org/10.1109/SCC.2017.70.

[31] Kaushik A, Gahletia S, Garg RK, Sharma P, Chhabra D, Yadav M. Advanced 3D body scanning techniques and its clinical applications. In2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO) 2022 Dec 23 (pp. 352-358). IEEE.

[32] Sicari S, Cappiello C, De Pellegrini F, Miorandi D, Coen-Porisini A. A security-and quality-aware system architecture for Internet of Things. Information Systems Frontiers. 2016 Aug;18:665-77. DOI 10.1007/s10796-014-9538-x

[33] Sicari S, Rizzardi A, Miorandi D, Cappiello C, Coen-Porisini A. A secure and quality-aware prototypical architecture for the Internet of Things. Information Systems. 2016 Jun 1; **58**:43-55. https://doi.org/10.1016/j.is.2016.02.003.

[34] Singh K, Yadav M, Singh Y, Barak D. Reliability Techniques in IoT Environments for the Healthcare Industry. InAI and IoT-Based Technologies for Precision Medicine 2023 (pp. 394-412). IGI Global. DOI: 10.4018/979-8-3693-0876-9.ch023

[35] Kumar, S., Kumar, A. ., Parashar, N. ., Moolchandani, J. ., Saini, A. ., Kumar, R. ., Yadav, M. ., Singh, K. ., & Mena, Y. . (2024). An Optimal Filter Selection on Grey Scale Image for De-Noising by using Fuzzy Technique. International Journal of Intelligent Systems and Applications in Engineering, **12(20s)**, 322–330. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/5143

[36] Yadav M, Kumar H. Profit analysis of repairable juice plant. *Reliability: Theory & Applications*. 2024; **19(1(77))**:688-95.

[37] Singh, K., Yadav, M., Singh, Y., Barak, D., Saini, A., & Moreira, F. Reliability on the Internet of Things with designing approach for exploratory analysis. *Frontiers in Computer Science*, 2024, **6**:1382347. https://doi.org/10.3389/fcomp.2024.1382347

[38] Branco F, Moreira F, Martins J, Au-Yong-Oliveira M, Gonçalves R. Conceptual approach for an extension to a mushroom farm distributed process control system: IoT and blockchain. In New Knowledge in Information Systems and Technologies: **1 (2019)** (pp. 738-747). Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-16181-1_69.