International Journal of Computational Methods and Experimental Measurements
Vol. 11, No. 2, June, 2023, pp. 123-134
Journal homepage: http://iieta.org/journals/ijcmem

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

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

[1] Department of Computer Science & Engineering, UIET, M.D. University, Rohtak 124001, India
[2] Department of Computer Science & Engineering, Vaish College of Engineering, Rohtak 124001, India
[3] Department of Applied Sciences, Mathematics, UIET, M.D. University, Rohtak 124001, India
[4] Department of Finance and Banking, Faculty of Applied Sciences, Usak University, Usak 64200, Turkey

*Corresponding Author Email: ercan.ozen@usak.edu.tr

https://doi.org/10.18280/ijcmem.110207

Received: 20 May 2023
Accepted: 23 June 2023

Keywords:
IoT reference model, reliability, data acquisition module, ISABELA, RTT

ABSTRACT

Reliability analysis aims to assess the dependability and performance of a system over time, considering factors such as device failures, communication issues, and data integrity. By integrating taxonomy and reliability analysis, researchers can systematically analyze and enhance the reliability of IoT systems by addressing specific components and categories identified in the taxonomy. IoT based on its reliable applications is classified among various categories such as smart home devices, smart watches, electric vehicles with IoT capabilities, industrial, healthcare, agriculture, soil monitoring sensors, smart city infrastructure, environmental monitoring devices, and smart energy management devices. The need for a consistent taxonomy was one of the problems recognized and examined in this paper even though IoT management technology is developing. To examine the reliability analysis of IoT systems, we created a brand-new taxonomy for IoT gadgets that places a strong focus on administration. We have released a completely new IoT reliability RBD model analysis at different gateways and Round-Trip Time is to be analyzed. It features an aircraft for dependability. Our goal is to help administrators of networks, as well as designers, put processes in place that will analyze and enhance the reliability of IoT systems. To implement techniques to increase the IoT system's reliability, we may utilize the management capabilities to keep an eye on the devices. ChatGPT can act as the conversational interface for ISABELA. By integrating ChatGPT with ISABELA's functionality, users can have natural language conversations with ISABELA, making the interaction more intuitive and user-friendly. A use case study of ISABELA has enhanced the position of the CHATGPT system in the IoT system which increase the efficiency and reliability of IoT designs and networks.

1. INTRODUCTION

Internet of Things (IoT) is a network of actual physical items, including machinery, automobiles, appliances, and other things, that are equipped with sensors, software, and networking capabilities to gather and share data online. The reliability of Internet of Things (IoT) systems is crucial for their successful deployment and operation. However, evaluating the reliability of IoT systems poses unique challenges due to their complex and dynamic nature. Specifically, there is a need for parametric evaluation techniques that can effectively assess and quantify the reliability of IoT systems. Parametric evaluation techniques involve the analysis of system parameters and their impact on reliability. These techniques consider factors such as device failures, communication disruptions, data integrity, and system downtime. However, the current state-of-the-art in reliability evaluation for IoT systems lacks comprehensive and standardized parametric techniques tailored specifically to the IoT domain. The problem statement, therefore, is to develop and establish parametric evaluation techniques that effectively capture and quantify the reliability aspects of IoT systems. Table 1 explains the key challenges of IoT systems to ensure the reliability framework and design approach.

Security and administration are two of the features included in the IoT reference model. Security and dependability are closely related since we cannot consider a system to be reliable if it contains security issues. When a system's security weakens, it loses dependability is violated. In the current work, security is not boarded.

Furthermore, there is a strong correlation between the IoT reference model's management capabilities and degree of dependability. On the one hand, we must make sure that the management system is trustworthy. Additionally, using the information gathered from a management solution put in place to increase the IoT system's dependability, we could forecast its behaviours, making this a win-win situation [1-4]. Initially, we choose the Device Layer for analysis, where the dependability of fundamental IoT system components will be considered initially [5-7]. RBD represents the block diagram for reliability. It is a method of graphical representation used to simulate and assess the dependability of complicated systems. RBDs are frequently used to assess the dependability and availability of systems and pinpoint probable failure modes in a variety of sectors, including engineering, aerospace, automobile, including telecommunications. Figure 1 depicts the RBD of Primary IoT systems.

Table 1. Key challenges in IoT systems

Key Challenges	Brief Explanation
Identifying relevant system parameters	IoT systems consist of a wide range of interconnected devices, communication protocols, and data flows. Defining the relevant system parameters that influence reliability is critical but challenging due to the heterogeneity and complexity of IoT architectures.
Defining metrics and evaluation models	Developing suitable metrics and evaluation models that can accurately measure and assess the reliability of IoT systems is crucial. These models should consider various aspects such as failure rates, mean time between failures (MTBF), mean time to repair (MTTR), fault tolerance, and system availability.
Handling dynamic environments	IoT systems operate in dynamic and unpredictable environments, where device connections, network conditions, and data patterns can change rapidly. Parametric evaluation techniques should account for these dynamic factors and provide mechanisms to adapt the evaluation process accordingly.
Scalability and resource constraints	IoT systems often involve a large number of interconnected devices with limited resources, including computing power, memory, and energy. Parametric evaluation techniques should be scalable and capable of handling resource-constrained IoT environments.
Integration with IoT development lifecycle	The parametric evaluation techniques should seamlessly integrate with the IoT system development lifecycle, from design and testing to deployment and maintenance. This integration ensures that reliability evaluation is considered at each stage, enabling proactive measures to enhance system reliability.

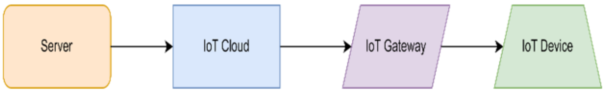

Figure 1. RBD of primary IoT systems

According to this diagram, the system consists of a server, an Internet of Things cloud, a gateway, as well as an IoT gadget. The parts are connected in a sequence. We need to segment the sensing process into two components to analyze the reliability of sensing: data collection and processing [6-10]. Figure 2 depicts the modules of a sensing.

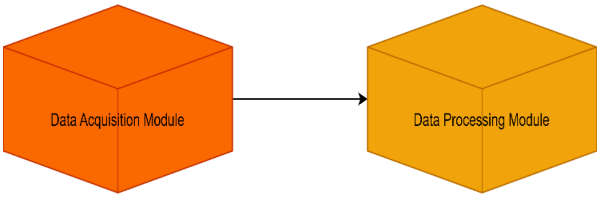

Figure 2. Modules of sensing reliability of IoT systems

The reliability of IoT systems shows acquisition is capturing the data in that module and processing the sets into the futuristic thing.

The modules are linked together in the sensing process as serial components. The next formula holds if each component's failure event occurs independently of the others, where $P\{E_i\}$ is the probability related to the event E_i that signals module i is operational, could be used to calculate the chance that both sections are operational.

$$P\{\text{Process}\} = \prod_{i=1}^{n} P\{E_i\} \tag{1}$$

from i=1 to n it variates.

The reliability of this Sensing layer is the summation of both the Reliability of Data acquisition and Data processing module. The addition of parallel redundancy in the system's components may increase its dependability [11-15]. We focus on an IoT system with redundant gateways (Figure 3). If we assume complete active redundancy no repair, the system must be seen as a parallel arrangement since, and in this case, parallelization provides redundancy and compares the dependability functions of each system [16-20]. The increase in percent between the two functions is also shown on the secondary axis, where the values are flipped for simpler presentation [21-25]. As we can see, using redundancy improves an IoT system's dependability when each component has a poor reliability rating of a greater amount [26-31].

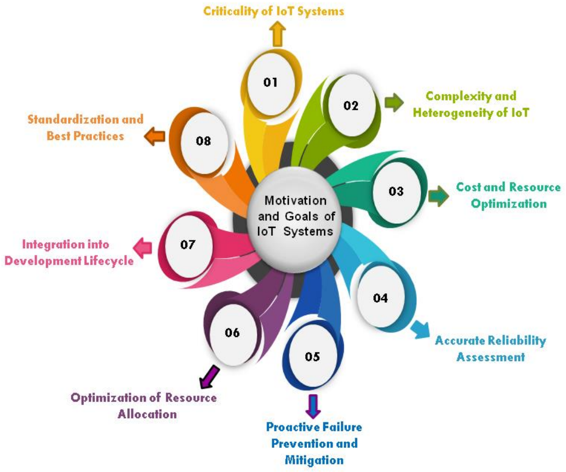

Figure 3. Motivation and goals of IoT systems

To formalize RBD combinations made up of type operators like series, parallel, and atomic, researchers define a recursive datatype named RBD. The corresponding dependability event is then returned by constructing an RBD datatype semantic function that is capable of decoding the RBD configuration supplied by these type constructors. Due to a system or part not failing within a particular period, this reliability event occurs [32-35]. Any combination of parallel as well as series RBD configurations may be accepted with ease by the suggested formalization technique since it is compositional by nature [36-39]. It also overcomes the drawbacks of series RBD formalizing by enabling us to investigate the general reliability formulations for RBDs on reliability occurrences lists of arbitrary length [40-42]. To further illustrate the compositional possibilities, we also give a higher-order logic encoding of a layered series-parallel RBD, specifically a series-parallel RBD having each block itself representing a series-parallel RBD arrangement of the suggested RBD formalization [43, 44]. The motivation and goals of developing parametric evaluation techniques for the reliability of IoT systems have been depicted in Figure 3. Also, it contributes to successful deployment, operation, and improvement of resilience in various domains.

The graphical diagrams established component configurations. The following are categorizations and descriptions of the redundancy categories offered by RBD: Series. The most basic setup for an RBD is a series [45-47]. There is no redundancy in a system linked in series, and for the system to work properly, each component connected in series must be in operation. A remote control (RC) helicopter, a personal computer (PC), and a smartphone are a few instances of series systems. Table 2 represents a systematic and structured literature review of IoT in reliability and RBD model with research gap and future scope.

In a parallel configuration, all components are active at all times in a configuration known as a k-out-of-n arrangement, but the system only needs the given number (k) of the entire number of components (n) to function. Simple backup units are available to take over in this sort of redundancy if certain numbers are exceeded or components fail. When two components are incorporated in the machine in a side-by-side arrangement and are both running, it is a scenario of parallel redundancy. The second component is one hand to take over if the first component fails since only one is necessary for the effective functioning of the system.

A commercial twin-engine aircraft that is designed to keep flying in the case of one engine failure is a practical illustration of a parallel system. Components in a standby setup are either marked as active or spare units. The spare components are ready to take over if any of the active units fail, much like a parallel setup. In standby systems, when only a certain amount (k) out of a total quantity (n) is necessary for the system to function, a comparable k-out-of-n relationship may exist. Standby systems also provide consideration to switching delays and breakdowns. Based on the failure patterns of the spare units, standby setups may be divided into many categories. Most literature depends on the experimental approach, whereas others need to be done through analysis.

Table 2. A systematic literature review of IoT in reliability and RBD model with research gap and future scope

Title of Paper	Author Names	Proposed Work	Future Scope	Research Gap
RelIoT: Reliability simulator for IoT networks. In the Internet of Things-ICIOT (2020)	Ergun et al.	It is an integrated reliability framework implemented in the ns-3 simulator, which enables reliability analysis at an early design phase for IoT networks.	An integrated reliability framework called RelIoT for IoT networks is used for other network simulators like OMNET+ etc.	RelIoT framework accurately models the power, temperature, and reliability dynamics of IoT devices. RelIoT enables reliability analysis at an early design phase, but we need more constructive solutions at a later stage as well.
IoT reliability: A review leading to five key research directions (2021)	Moore et al.	The ability to quantify the reliability of IoT devices, systems and network is a critical function.	These solutions will require more experimental work to strengthen and support the reliability of our IoT infrastructure, resulting in a safer and more stable paradigm for its users.	For quantifying dependability in the IoT, reliability highlights the many difficulties involved in this job. Several important research objectives for IoT. Less experimental work is shown to emerge in an immersive way.
Reliability for emergency applications in the Internet of Things (2013)	Maalel et al.	This paper focuses on the reliability of emergency applications under IoT technology, ensuring high-priority events are delivered without packet loss.	Proposed reliable protocol for data transmission in IoT. Future work includes evaluating protocol effectiveness and examining probabilistic models.	Needs to add more research on Emergency Case Studies with their applications.
Reliability in the Internet of Things: Current status and future perspectives (2020)	Xing	Research on the reliability of the Internet of Things is in its early stages.	Upcoming new features of increasing IoT infrastructure complexity as well as dynamics, challenging research concerns, and prospects are highlighted and can be used in future.	Mathematical Equations but lacks reliability in experiments.
Simulating reliability of IoT networks with RelIoT (2020)	Ergun et al.	The power, temperature, and reliability characteristics of actual networked IoT devices are faithfully captured by RelIoT.	Using our framework, we can show that RelIoT successfully models the reliability, power, and overall temperature dynamics of actual networked IoT devices for more applications.	It lacks the essence of parameters for IoT.
An end-to-end reliability framework of the Internet of Things (2020)	Azghiou et al.	The suggested framework is flexible, expressive, and highly scalable.	The numerical investigation provides mission time intervals that describe an IoT system's behavior from the perspective of its dependability.	More approaches for different RBD models can be used.
End-to-end reliability analysis of IoT-based smart agriculture (2018)	Kamyod	The simulation results show exciting reliability features of the intended IoT communication architecture.	Simulation results show exciting reliability features of the intended IoT communication architecture through main reliability network parameters by using OPNET.	Need to add more Simulators to add on features and work for the reliability of the IoT.

Several research gaps have been identified from the literature review of past studies which can be fulfilled from this research work. Current reliability models for IoT systems often assume static conditions and do not consider the dynamic nature of IoT environments. Investigating techniques that can dynamically update RBDs or reliability models based on real-time data and environmental changes would be beneficial. IoT systems often involve data fusion and processing at various stages, including data aggregation, filtering, and analytics. IoT reliability assessment, through our study considering the interdependencies and interactions between IoT devices and the physical world, has been done. Research gaps exist in understanding the reliability implications of integrating diverse IoT components and addressing the heterogeneity in reliability modeling and analysis. By addressing these research gaps, researchers can contribute to advancing the understanding and practice of IoT reliability and reliability analysis using RBDs. Closing these gaps will ultimately lead to the development of more robust, resilient, and dependable IoT systems.

In conclusion, the introduction provides an overview of the existing literature on IoT reliability and the utilization of Reliability Block Diagram (RBD) models for analysis. It emphasizes the criticality of reliability in IoT systems, given their increasing deployment in mission-critical domains. The introduction highlights the challenges specific to IoT reliability analysis, including the dynamic nature of IoT environments, resource constraints, and heterogeneity. The study's importance lies in addressing these challenges and bridging the identified research gaps. By providing a structured review of the literature, this study aims to advance the understanding of IoT reliability and RBD models, facilitate standardization, and guide future research and industry practices. The study's outcomes will contribute to enhancing the reliability of IoT systems, ensuring their dependable operation, and enabling the seamless integration of IoT technologies into diverse applications and domains.

2. RELIABILITY BLOCK DIAGRAMS FOR REDUNDANCY GATEWAYS

Blocks and connection lines make up the visual structures known as reliability block diagrams (RBDs). The connector lines indicate how the blocks link the system components, which are often represented as blocks. If there is at least one route of correctly working components from input to output, the system operates properly; otherwise, it malfunctions.

Any one of these three primary component connection patterns-series, active redundancy, or standby redundancy-can be employed in an RBD architecture. The system's components must all function properly. Active redundancy, as opposed to passive redundancy, calls for the complete operational functioning of every component in at least one alternative stage. The parts of an active redundancy may be connected by a parallel organization. All components don't need to be active in a standby redundancy. One must be aware of the functional interconnections between the system's components, the dependability of each component, and the mission durations during which reliability is needed to construct the RBD of a specific system. The design engineers utilize this information to identify the best RBD architecture (series, parallel, or series-parallel) and assess the system's overall reliability. Figure 4 depicts the reliability of the IoT RBD diagram of the redundancy of gateways.

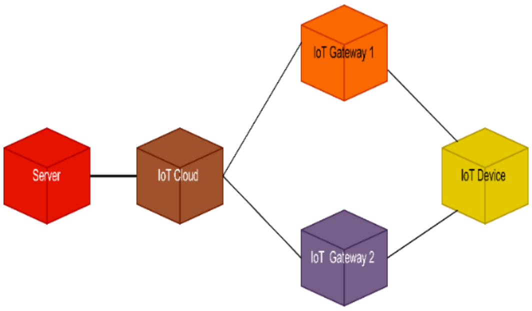

Figure 4. Reliability of IoT RBD diagram of redundancy of gateways

3. REDUNDANCY WITH SENSORS AND FUNCTIONALITY

The fundamental structure of the IoT network was tested. A personal PC serves as the database and web server for our system. The FI-WARE platform is installed over these services. The Arduino Uno is a metaphor for any embedded system that conducts data collection via sensors, but which lacks functionality for wireless communications, necessitating the need for a gateway to transfer data to a server.

We used digital temperature as well as humidity sensors-more precisely, DHT11 sensors—for our testing. Digital inputs were used to link the sensors to an Arduino Uno, and the DHTLIB library (Arduino Foundation, 2018) was used to transfer data. To receive the data after it was collected, a Raspberry Pi 3 remained cast off as a gateway device. This joining made use of the I2C bus protocol. All of the information received from the sensors was then sent to the server via the Raspberry Pi over a Wi-Fi or Ethernet network. A round trip time was recorded for each sensor's information reply that was obtained. The local clock of the computer counted the amount of time between the moment a request left the server and the moment its reply arrived. TCP stands for Transmission Control Protocol. It is one of the core protocols of the Internet Protocol Suite, commonly known as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of data between applications running on devices connected to a network. Using TCP connections, Python software carried out this request. For the primary and backup connections, respectively, we specified two sockets.

Because the Raspberry Pi runs the Linux operating system, a sudden power interruption may cause issues when the device is restarted, resulting in the loss of service. Additionally, issues with communication lines may result in service interruptions. On the previously described idea of redundancy, we created methods that increased the system's resilience in this context. In our dependability case studies, we specifically considered the device and connection redundancies.

When a connection fails, the socket locks during the default timeout, the TCP port stalls, and the connection is abruptly lost. It is required to force its closure rather than wait for the default timeout to run out. For this, a flag the client program was activated, and then the reconnection phase began.

Round Trip Time (RTT) is a networking term that refers to the time it takes for a data packet to travel from the source to the destination and then back to the source again. We estimated the typical RTT under ideal conditions (i.e., no issues) for each test scenario. The measurements were made ten times each, spaced four minutes apart. We measured RTT more than 110 times throughout each test cycle, depending on how long it took for communication to restart on the backup connection.

The average RTT was then determined for each scenario with a 95% confidence level. These outcomes are shown in Table 1. The average RTT values degrade in the majority of situations.

Even when there are connection or device failures, there is only a very tiny increase, demonstrating the success of the suggested dependability measures.

In addition, the last column of Table 3 displays the average maximum RTT for the test period, under typical circumstances like those in the four scenarios. As can be seen, link redundancy results in much lower values of this parameter (i.e., (b), (c), and (d)).

Table 3. Average RTT(S)

Scenario	Average of Max. RTT(s)	Confidence	Interval
Normal conditions	394.518	104.8	1593.83
Scenario (a)	450.797	151.84	1669.59
Scenario (b)	401.643	94.02	639.16
Scenario (c)	410.894	91.43	584.80
Scenario (d)	399.610	89.19	800.25

Additionally, Table 4 shows that scenario (a) had the largest increase in average RTT while failure circumstances were used, increasing by 14.27%, while scenario (d) had the smallest increase, demonstrating once more the relative superiority of link redundancy across device redundant storage.

Table 4. Average RTT increases respect

Scenario	Normal Conditions (us)	% of Average RTT Increase
Scenario (a)	56.28	14.27
Scenario (b)	7.12	1.58
Scenario (c)	16.38	4.08
Scenario (d)	5.09	1.24

The results obtained unmistakably indicate certain deductions with the Internet of Things. First, it is possible and efficient to provide dependency via redundant IoT devices, links, or both. Second, the cost of performance is rather low. Finally, the efficacy of the entire infrastructure is not noticeably hindered by deploying devices like Fog-Phones to provide connection dependability. If one understands that these devices may provide local processing as well as local storage features in addition to connection redundancy, it could even pay off. ISABELA stands for IoT Student Advisor & Best Lifestyle Analyzer. Internet of Things student advisor refers to a system or application that utilizes IoT technology to provide guidance and support to students. This can be achieved through various means, such as smart devices, sensors, and data analysis. The goal of the case study is to implement a system that enables the monitoring of factors linked to students' lifestyles and the environments in which they work and learn. The information gathered is then linked to their academic standing. Figure 5 depicts the ISABELA networking with the Internet of Things.

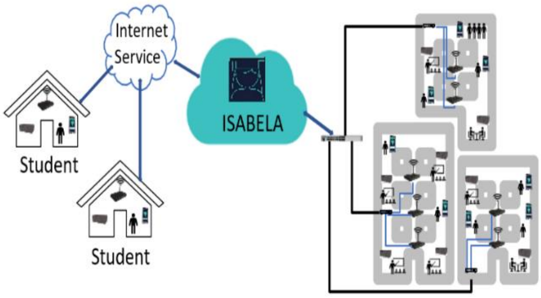

Figure 5. ISABELA Networking with the Internet of Things [48]

3.1 Stress awareness

In the IoT Student Advisor & Best Lifestyle Analyzer case study, one of the key aspects focused on stress awareness among student volunteers. Recognizing the prevalence of stress among students and its impact on their overall well-being, the IoT system was designed to monitor and analyze stress levels using various sensors and data inputs. The study involved a group of student volunteers who wore IoT devices equipped with physiological sensors such as heart rate monitors, skin conductance sensors, and sleep trackers. These devices collected real-time data on the students' physiological responses, activity levels, and sleep patterns. The collected data was then processed and analyzed by the IoT system, providing insights into the students' stress levels and identifying potential triggers. By leveraging the power of IoT and data analytics, the IoT Student Advisor & Best Lifestyle Analyzer(ISBELA) system aimed to provide personalized recommendations and interventions to help students manage and reduce their stress levels. These recommendations included techniques such as mindfulness exercises, relaxation techniques, physical activity suggestions, and sleep optimization strategies. The study not only provided valuable insights into the stress levels of the student volunteers but also highlighted the potential of IoT systems in promoting stress awareness and well-being in educational settings. It demonstrated the feasibility of using IoT devices and data analytics to monitor and analyze stress levels in real time, providing personalized support and interventions for stress management. The findings of the study emphasized the importance of stress awareness and the potential benefits of integrating IoT technologies into student support systems. By addressing stress proactively, educational institutions can better support the mental health and well-being of their students, ultimately enhancing academic performance and overall quality of life. The "Stress Awareness" subsection of the IoT Student Advisor & Best Lifestyle Analyzer case study highlights the significance of using IoT devices and data analytics to monitor and manage stress levels among students. It showcases the potential of IoT systems in providing personalized support and interventions, contributing to stress reduction and improved well-being in educational environments. In reliable data on stress levels, analyze the data using advanced techniques, and provide personalized insights and recommendations for stress management. The combination of quantitative physiological data and qualitative feedback from participants allowed for a holistic understanding of stress patterns and effective interventions for stress reduction and overall well-being.

3.2 Data acquisition

Data Acquisition and processing make up the two steps of sensing in the current situation. The initial stage of data gathering is where trustworthy data must be gathered. Reliability is essential in important applications where there is a potential danger to human life, such as health monitoring. Processing data is the second stage.

In this situation, we choose to employ an academic scenario to investigate the validity of the data collection procedure and to get information on student behavior before a test or assessment regarding stress or anxiety. ECG (Electrocardiogram) and BVP (Blood Volume Pulse) sensors are commonly used for data gathering in various fields, including healthcare, sports, and research. These sensors provide valuable information about the electrical activity of the heart and blood flow patterns, respectively and we utilize a Biosignalsplux package with ECG and BVP sensors.

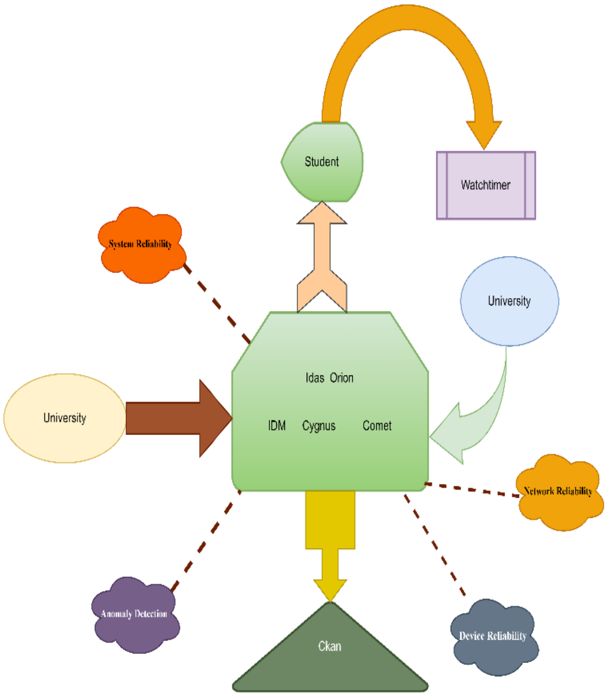

Figure 6. IoT data capturing nodes and types of reliability cognizance

The above Figure 6 shows the IoT Data Capturing nodes and types of Reliability Cognigance. University Students capture data points with their nodes and reliability measures for themselves. Four types of Reliability Measures will find an effective way of assurance that all the nodes are congruent toward the chain of accuracy and precision.

Twenty University of Coimbra student volunteers-two women and eighteen men ranging in age from 19 to 27 were used to compile a dataset. Five minutes were spent on the measures in two stages: just before the assessment event and just after it. Every participant has already consented to the use of the data gathered before the commencement of the measuring process.

The measurements were collected by a Biosignalsplux study, in which each student's left thorax was used to monitor the ECG using a local differential triode. The student's index finger was where the BVP sensor was placed.

The latest string of chromosomes is produced for each generation by continued crossover and mutation of the population's chromosome, which is one string of the population. One generation refers to this series of actions, including reproduction, crossover, and mutation. Following mutation, each new string in the population is referred to as a "child string," which then serves as the parent string for the following generation. This is carried out repeatedly unless the mean fitness squared error of the strings is minimized [49-51].

4. IMPLEMENTATION OF CASE STUDY FOR RELIABILITY OF IOT SYSTEMS

The insights gained from analyzing the system's reliability, performance, scalability, interoperability, security, and privacy aspects contribute to a comprehensive understanding of the challenges and considerations in ensuring reliable IoT systems. The implemented system can be used as a test bed to evaluate the reliability of IoT systems. By monitoring and analyzing the performance and behavior of the IoT devices, data acquisition and integration processes, data processing and analysis techniques, and user interface interactions, researchers can assess the reliability aspects of the system. The findings from the system implementation can provide empirical evidence and real-world data to support the conclusions on the reliability of IoT systems.

The implementation allows researchers to measure and evaluate the performance of the IoT Student Advisor & Best Lifestyle Analyzer system. Parameters such as response time, data processing efficiency, and scalability can be analyzed to assess the system's performance. The IoT Student Advisor & Best Lifestyle Analyzer system exemplifies several aspects that contribute to the overall reliability of IoT systems, making important connections to the broader context of IoT reliability.

An IoT-based case study is called Student Mentor & Best Behaviour Analyser (ISABELA). The objective of this case study aims to put a system into place. that enables the tracking of characteristics of students' lifestyles and the settings in which they work and learn. The information gathered is then linked to their academic standing. ISABELA's platform was developed using the HiLCPS idea. It is made up of several interconnected components.

To gather data on the users' daily lives, ISABELA leverages the sensors in smartphones as well as additional virtual sensors (like social network interactions) and various physical sensors, such as those for light, sound, temperature, as well as humidity.

The IoT Student Advisor & Best Lifestyle Analyzer system can be implemented using the FIWARE platform, which provides a set of open-source components and standards for building scalable and interoperable IoT applications. Here's an overview of how the system can be implemented using FIWARE:

1) Data Acquisition and Device Integration: IoT devices equipped with physiological sensors, such as heart rate monitors, skin conductance sensors, and sleep trackers, can be connected to the FIWARE platform. FIWARE provides standardized protocols and APIs (e.g., MQTT, CoAP) to facilitate seamless integration and communication between the IoT devices and the platform.

2) Device Context Broker: The FIWARE Context Broker component can be used to manage and store real-time data streams from IoT devices. It acts as a centralized repository for collecting and managing the data.

3) Data Processing and Analysis: The Orion Context

Broker component in FIWARE can be used to process and manage the collected data. It provides functionalities for data filtering, aggregation, and enrichment.

4*) Data Analysis Tools:* FIWARE offers various tools and frameworks, such as the FIWARE Data Visualization tool and FIWARE Machine Learning (ML) libraries, to perform advanced data analysis on the collected physiological data.

5) ML Algorithms: FIWARE ML libraries can be utilized to develop predictive models or anomaly detection algorithms that analyze the physiological data and provide insights into stress levels and patterns.

6) User Interface Development: The FIWARE platform supports the development of web-based dashboards and mobile applications through its User Interface Management (WireCloud) component.

7) Personalized Recommendations: Based on the data analysis, the FIWARE system can generate personalized recommendations for stress management, leveraging the analyzed physiological data and ML models. These recommendations can be presented to users through the user interface.

8) Security and Privacy: FIWARE provides security mechanisms, such as OAuth2-based authentication and authorization, to ensure secure data exchange and access control within the system. Privacy policies and consent management can be implemented using FIWARE's PEP Proxy and Authorization PDP components, allowing users to control the usage and sharing of their data.

Integration with External Services:

The FIWARE platform offers a wide range of standardized APIs and connectors to integrate with external services, such as fitness trackers, weather data providers, or educational platforms. These integrations can enrich the IoT Student Advisor & Best Lifestyle Analyzer system with additional contextual information, enabling a more comprehensive analysis and personalized recommendations.

By leveraging the capabilities of the FIWARE platform, the IoT Student Advisor & Best Lifestyle Analyzer system can be implemented in a scalable, interoperable, and secure manner. FIWARE's standardized components and APIs simplify the development process and facilitate seamless integration with IoT devices, data analysis tools, user interfaces, and external services, enabling a robust and efficient implementation of the system.

Implementing the IoT Student Advisor & Best Lifestyle Analyzer system using the FIWARE platform offers several benefits that enhance its performance, scalability, and interoperability with other IoT platforms:

1) Performance Improvement: FIWARE provides a scalable and distributed architecture that allows the system to handle a large volume of data from IoT devices without compromising performance. The platform's components, such as the Context Broker and Data Visualization tool, are designed to efficiently process and manage real-time data streams, ensuring fast and responsive performance. Additionally, FIWARE offers caching mechanisms and load-balancing techniques, enabling the system to handle high traffic loads and optimize resource utilization.

2) Scalability: The FIWARE platform is built with scalability in mind, allowing the IoT Student Advisor & Best Lifestyle Analyzer system to easily scale horizontally or vertically as the number of IoT devices and users increases. The platform's architecture supports the deployment of additional instances of components to handle increased data processing and user demands. With FIWARE, the system can dynamically scale resources, ensuring efficient utilization of hardware and cloud infrastructure, and enabling seamless expansion to accommodate growing user bases.

3) Interoperability with Other IoT Platforms: FIWARE follows open standards and APIs, enabling interoperability with other IoT platforms and services.

The platform's standardized protocols, such as MQTT and CoAP, facilitate easy integration with IoT devices from different manufacturers and communication protocols. FIWARE's components can also interact with external services and platforms through its standardized APIs, allowing seamless data exchange and integration with third-party systems.

4) Data Integration and Fusion: FIWARE's Context Broker component provides a central repository for managing and integrating data from diverse IoT devices and sources.

The platform allows for the integration of data from various sensors, fitness trackers, educational platforms, or other external services, providing a holistic view of users' lifestyles and well-being. By integrating and fusing data from multiple sources, the system can generate more comprehensive insights and personalized recommendations for stress management.

5) Security Mechanisms: FIWARE offers robust security mechanisms, including authentication, authorization, and data encryption, ensuring the privacy and integrity of sensitive user data. The platform's security features protect the IoT Student Advisor & Best Lifestyle Analyzer system from potential security threats, safeguarding user information and maintaining data confidentiality.

For the mentioned project, the activities for storing and processing data are located on a server that is part of the FIWARE Platform that is being used to develop it. Smartphones that run the ISABELA program, which gathers data collected by students' microphone, light sensor, proximity sensor, mobile cell phone lock, GPS, gyroscope, Wi-Fi, and Bluetooth signals, statistics of calls. An Internet of Things (IoT) box put in the classrooms, cafeteria, and dorm rooms for the students. It has an Arduino Uno module, a Raspberry Pi 3 microprocessor, and sensors for humidity, sound, temperature, and sunlight, as well as three pieces of network equipment [52-55].

We created a specialized box utilizing Autodesk 123D Design to ensure dependable data collection using the IoT box. It was then prepped for 3D printing using Ultimaker Cura. The design considered the use of four sensors: temperature, humidity, sound, and light. The light sensor was put on top of the box, and the sound, temperature, and humidity sensors were all positioned on the same side of the box. For connecting the power supply, interfaces for networks, and video interface, we also took into account the many USB ports onboard the Raspberry Pi 3 and Arduino Uno. Figure 5 illustrates the finished box along with its connections.

The IoT box's main function is to collect data about the student's home and the university where he or she attends lessons. In this instance, the ISABELA box's data-collecting procedure makes use of sensors for light, sound, humidity, and temperature. An analog/digital converter was necessary since several of the sensors use analog signals. “This process was implemented on an Arduino Uno, with each sensor connected to either digital or analog ports. Data is sent from the data collecting device to the IoT Cloud using a Raspberry Pi 3 acting as an IoT gateway. We gather information on the pupils' physical activity, location, sleep, emotions, and sociability to determine goals and infer their behavior.

Three distinct categories of sources were used throughout the data-collecting process:

1) Mobile Phone Sensors: Using information from WiFi scans and GPS, we were capable of locating and tracking students using the accelerometer and gyroscope detectors in their phones. For the sleep state, we employed the light, proximity sensors, alarm information, phone lock, and microphone. Last but not least, to assess how near other devices were, we used data on the number of SMSs sent and received, calls made, received, and lost; b) the duration of these calls; the range of destinations of the calls / SMS; as well as c) Bluetooth proximity data.

2) Questionnaire: The students provided daily information on their emotional condition, amount of study time, sleep quality, and overall sociability using an application-integrated questionnaire.

3) Social Networks: To determine a person's emotional state, we used what they post on social networks such as Twitter and Facebook, including their comments and the number of times they were retweeted.

To improve reliability, we used fusion sensor techniques in the setting of mobile phone sensors [56-60].

Three modules are used on the cellphone to process the data:

1) Physical Activity: Using Google's Activity Recognition API, we deduced the student activity that could be classified in one of the following five states exercise, walking, stationary, in a vehicle, and undetermined.

2) Location: The university, the house, and other sites were listed as the three locations. To locate the student inside, we primarily use a collection of the SSIDs of the available WiFi networks (because we could anticipate the SSIDs of the respective networks, it was easy to tell whether the child was at home or the university). If the GPS function on the mobile phone was on, we also used this information. When the GPS data was analyzed, the position was designated as being within a 200-meter perimeter of the Faculty of Electric and Electronic Engineering "University."

3) Sociability: Data on the volume of SMS sent as well as received, the number of calls made, answered, as well as dropped, the duration of the calls, and the volume of different SMS and call destinations were used to create this categorization.

Improving the reliability of IoT fusion sensor techniques in the setting of mobile phone sensors involves several key considerations [61-63]. By implementing sensor calibration, advanced fusion algorithms, redundancy, data validation, energy efficiency optimizations, edge computing, security measures, and continuous testing, it can enhance the reliability of sensor data in mobile phones for IoT applications [64-66]. These measures collectively ensure accurate and dependable sensor readings, leading to improved performance and user experience in the IoT ecosystem.

The FIWARE platform has been developed as a modular framework to offer a standard suitable for IoT platforms over Europe [67] and is utilized to put ISABELA into practice while processing takes place on the cloud.

To meet the demands of various IoT platforms, FIWARE offers a variety of Generic Enablers (GE). Five of these GEs—the ORION, the CYGNUS, the STH COMET, and the IDAS, besides the KEYROCK—remain used in our implementation of the FIWARE. Throughout its entire lifecycle, the ORION manages context information using an NGSIv2 REST API. Figure 7 depicts the access point of servers at different internet service Providers with IoT device.

Additionally, ORION is capable of managing subscriptions that include contextual data and offering sophisticated data filtering. Another GE offering a RESTFUL API with historic-query capabilities, including aggregating techniques, is The Short-Term-History, or STH-Comet. Each Comet GE will be connected to MongoDB to get the data anytime the ISABELA application needs to retrieve earlier data. It is possible to link the ORION with IDAS to combine IoT devices into physical items. A particular sensor of an IoT device may be linked to a property of a thing specified in ORION. As a result, several entities may connect to a set of sensors or even the same detector simultaneously. The CYGNUS facilitates coordination as well as encourages communication among the many components. To protect data from unwanted access, the KEYROCK also handles user IDs and acts as the system's identity component.

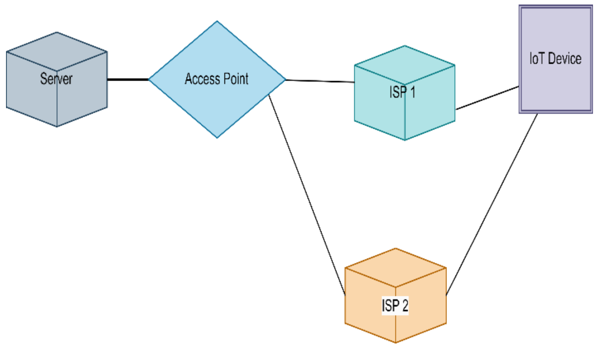

Figure 7. The access point of servers at different Internet service providers with IoT device

Implementation of the IoT Student Advisor & Best Lifestyle Analyzer system involves several key components and techniques to ensure its functionality and effectiveness. Researchers can analyze how the system handles a growing number of IoT devices, data streams, and user interactions, examining the scalability of the system. The interoperability features of the implemented system can be evaluated by integrating external services or IoT platforms, providing insights into the challenges and benefits of interoperability in ensuring reliability. The findings related to scalability and interoperability can inform the conclusions on the significance of these aspects for the overall reliability of IoT systems. The implementation of security mechanisms and privacy policies in the system allows researchers to evaluate the effectiveness of these measures in ensuring the reliability of IoT systems. By conducting security assessments, penetration testing, and privacy impact assessments, researchers can identify vulnerabilities and risks that may affect the reliability of the system. The findings regarding the security and privacy aspects can contribute to the conclusions on the importance of robust security measures for reliable IoT systems and the potential risks associated with data breaches or unauthorized access. In summary, the implementation of the IoT Student Advisor & Best Lifestyle Analyzer system using the discussed components and techniques provides an empirical basis for the findings and conclusions of the study on Parametric Evaluation Techniques for the Reliability of IoT. The insights gained from analyzing the system's reliability, performance, scalability, interoperability, security, and privacy aspects contribute to a comprehensive understanding of the challenges and considerations in ensuring reliable IoT systems

5. CONCLUSIONS

This paper presents the solutions integrating with experimental results of An IoT system that has a reliability plane with a set of redundancy of gateway with the results showing average round trip time is how much changes in different Scenarios (a), (b), (c) and (d) and also used to normalize the average time increase in different planes. Management plane incorporated into it may monitor network performance, identify errors, collect failure metrics, and set settings, giving it control over the system's capabilities. Therefore, the major goal of this effort was to Include an internet administration interface that manages the various ISABELA system components. Consequently, The operational data gathered might be utilized for improving platform reliability. This has the effect of enhancing the usage of IoT Systems in access points of ISPs for more effective reliability. Various limitations have been taken in the study such as specificity of the evaluation techniques, sample size and diversity, time constraints and long-term reliability, and evolving technology landscape. Factors such as hardware configurations, software versions, and network conditions specific to the implementation may impact the observed reliability outcomes. To enhance the generalizability and applicability of the findings, future research should consider larger and more diverse samples, evaluate multiple implementations, account for long-term reliability, and explore different IoT contexts. Additionally, ongoing research and collaboration with industry stakeholders can address the evolving technology landscape and ensure the findings remain relevant as IoT systems continue to advance.

Based on the findings and limitations of the study on parametric evaluation techniques for the reliability of IoT, there are several possible directions for future research. Assess the effectiveness of these techniques in mitigating failures, improving fault recovery, and increasing system resilience. Investigate the impact of different network conditions, such as network congestion, intermittent connectivity, and high latency, on the reliability of IoT systems. Analyze how varying network conditions affect data transmission, system responsiveness, and overall reliability. By exploring additional techniques, considering diverse network conditions and environments, evaluating solutions in different domains, assessing long-term reliability, incorporating user perspectives, and leveraging AI, researchers can further enhance the reliability and resilience of IoT systems in various application contexts.

ACKNOWLEDGEMENT

This work is supported by the UIET, M.D. University, Rohtak.

REFERENCES

[1] Ergun, K., Yu, X., Nagesh, N., Cherkasova, L., Mercati, P., Ayoub, R., Rosing, T. (2020). RelIoT: Reliability simulator for IoT networks. In Internet of Things-ICIOT 2020: 5th International Conference, Honolulu, HI, USA, September 18-20, 2020. https://doi.org/10.1007/978-3-030-59615-6_5

[2] Moore, S.J., Nugent, C.D., Zhang, S., Cleland, I. (2020). IoT reliability: A review leading to 5 key research directions. CCF Transactions on Pervasive Computing and Interaction, 2: 147-163. https://doi.org/10.1007/s42486-020-00037-z

[3] Yadav, M. (2020). A review on piezoelectric energy harvesting systems based on different mechanical structures. International Journal of Enhanced Research in Science, Technology & Engineering, 9(1): 1-7.

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

[5] Xu, Z., Saleh, J.H. (2021). Machine learning for reliability engineering and safety applications: Review of current status and future opportunities. Reliability Engineering & System Safety, 211: 107530. https://doi.org/10.1016/j.ress.2021.107530

[6] Xing, L., Tannous, M., Vokkarane, V.M., Wang, H., Guo, J. (2017). Reliability modeling of mesh storage area networks for Internet of Things. IEEE Internet of Things Journal, 4(6): 2047-2057. https://doi.org/10.1109/JIOT.2017.2749375

[7] Maalel, N., Natalizio, E., Bouabdallah, A., Roux, P., Kellil, M. (2013). Reliability for emergency applications in Internet of Things. In 2013 IEEE International Conference on Distributed Computing in Sensor Systems, Cambridge, MA, USA, May 20-23, 2013. https://doi.org/10.1109/DCOSS.2013.40

[8] Xing, L. (2020). Reliability in Internet of Things: Current status and future perspectives. IEEE Internet of Things Journal, 7(8): 6704-6721. https://doi.org/10.1109/JIOT.2020.2993216

[9] Rajawat, A.S., Bedi, P., Goyal, S.B., Shaw, R.N., Ghosh, A. (2022). Reliability analysis in cyber-physical system using deep learning for smart cities industrial IoT network node. AI and IoT for Smart City Applications, 157-169. https://doi.org/10.1007/978-981-16-7498-3_10

[10] Sandelic, M., Peyghami, S., Sangwongwanich, A., Blaabjerg, F. (2022). Reliability aspects in microgrid design and planning: Status and power electronics-induced challenges. Renewable and Sustainable Energy Reviews, 159: 112127. https://doi.org/10.1016/j.rser.2022.112127

[11] Li, X.Q., Song, L.K., Bai, G.C. (2022). Recent advances in reliability analysis of aeroengine rotor system: A review. International Journal of Structural Integrity, 13(1): 1-29. https://doi.org/10.1108/IJSI-10-2021-0111

[12] Kholmirzayev, S., Akhmedov, I., Khamidov, A., Akhmedov, A., Dedakhanov, F., Muydinova, N. (2022). Calculation of reinforced concrete structures of buildings based on the theory of reliability. Science and Innovation, 1(A8): 1027-1032. https://doi.org/10.5281/zenodo.7447650

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

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

[15] Yadav, M., Kumar, S., Kaushik, A., Garg, R.K., Chhabra,

D. (2023) 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, 71(2): 296-314. https://ijettjournal.org/Volume-71/Issue-2/IJETT-V71I2P232.pdf

[16] Su, M.Y. (2011). Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers. Expert Systems with Applications, 38(4): 3492-3498. https://doi.org/10.1016/j.eswa.2010.08.137

[17] Kou, G., Yi, K., Xiao, H., Peng, R. (2022). Reliability of a distributed data storage system considering the external impacts. IEEE Transactions on Reliability, 72(1): 3-14. https://doi.org/10.1109/TR.2022.3161638

[18] Hulme, A., Stanton, N.A., Walker, G.H., Waterson, P., Salmon, P.M. (2022). Testing the reliability and validity of risk assessment methods in human factors and ergonomics. Ergonomics, 65(3): 407-428. https://doi.org/10.1080/00140139.2021.1962969

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

[20] Yeh, W.C., Tan, S.Y., Zhu, W., Huang, C.L., Yang, G.Y. (2022). Novel binary addition tree algorithm (BAT) for calculating the direct lower-bound of the highly reliable binary-state network reliability. Reliability Engineering & System Safety, 223: 108509. https://doi.org/10.1016/j.ress.2022.108509

[21] Metsämuuronen, J. (2022). Attenuation-corrected estimators of reliability. Applied Psychological Measurement, 46(8): 720-737. https://doi.org/10.1177/01466216221108131

[22] Yadav, M., Yadav, D., Kumar, S., Garg, R.K., Chhabra, D. (2019). Experimental & mathematical modeling and analysis of piezoelectric energy harvesting with dynamic periodic loading. International Journal of Recent Technology and Engineering, 8(3): 6346-6350.

[23] Herwin, H., Pristiwaluyo, T., Ruslan, R., Dahalan, S.C. (2022). Do scoring techniques and number of choices affect the reliability of multiple-choice tests in elementary schools? Cypriot Journal of Educational Sciences, 17(4): 1258-1268. https://doi.org/10.18844/cjes.v17i4.7149

[24] Abeshu, A., Chilamkurti, N. (2018). Deep learning: The frontier for distributed attack detection in fog-to-things computing. IEEE Communications Magazine, 56(2): 169-175. https://doi.org/10.1109/MCOM.2018.1700332

[25] Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen, S., Isoaho, J. (2016). Distributed internal anomaly detection system for Internet-of-Things. In 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, Jan. 9-12, 2016. https://doi.org/10.1109/CCNC.2016.7444797

[26] Zhang, R., Shim, B., Yuan, W., Di Renzo, M., Dang, X., Wu, W. (2022). Integrated sensing and communication waveform design with sparse vector coding: Low sidelobes and ultra reliability. IEEE Transactions on Vehicular Technology, 71(4): 4489-4494. https://doi.org/10.1109/TVT.2022.3146280

[27] Yadav, M., Yadav, D. (2019). Micro energy generation in different kinds of water flows on lead zirconium titanite/PVDF. International Journal of R&D in Engineering, Science and Managemeny, 9(5): 1-8.

[28] Najafzadeh, M., Homaei, F., Mohamadi, S. (2022). Reliability evaluation of groundwater quality index using data-driven models. Environmental Science and Pollution Research, 29(6): 8174-8190. https://doi.org/10.1007/s11356-021-16158-6

[29] Kamyod, C. (2018). End-to-end reliability analysis of an IoT based smart agriculture. In 2018 International Conference on Digital Arts, Media and Technology (ICDAMT), Phayao, Thailand, Feb. 25-28, 2018. https://doi.org/10.1109/ICDAMT.2018.8376535

[30] Ahlawat, A., Phogat, A., Yadav, M., Sahdev, R.K., Dhingra, A.K., Chhabra, D. (2023). Fabrication and analysis of ABS-HDPE-PC composite polymer filament used for FDM printing using hybrid algorithm. International Journal on Interactive Design and Manufacturing (IJIDeM), 1-11. https://doi.org/10.1007/s12008-023-01389-3

[31] Kazemi, M., Ansari, M.R. (2022). An integrated transmission expansion planning and battery storage systems placement-A security and reliability perspective. International Journal of Electrical Power & Energy Systems, 134: 107329. https://doi.org/10.1016/j.ijepes.2021.107329

[32] Kaushik, A., Punia, U., Garg, R.K., Yadav, M., Vashistha, R., Rathee, M., Sahdev, R.K., Chhabra, D. (2022). Optimization of process parameters for scanning human face using hand-held scanner. PREPRINT (Version 1) available at Research Square. https://doi.org/10.21203/rs.3.rs-2051093/v1

[33] Spanos, G., Giannoutakis, K.M., Votis, K., Tzovaras, D. (2019). Combining statistical and machine learning techniques in IoT anomaly detection for smart homes. In 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, Sep. 11-13, 2019. https://doi.org/10.1109/CAMAD.2019.8858490

[34] Afshari, S.S., Enayatollahi, F., Xu, X., Liang, X. (2022). Machine learning-based methods in structural reliability analysis: A review. Reliability Engineering & System Safety, 219: 108223. https://doi.org/10.1016/j.res/j.ress.2021.108223

[35] Yadav, M., Kumar, S., Kaushik, A., Chhabra, D. (2022). 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, 1-14. https://doi.org/10.1007/s40033-022-00440-z

[36] González-Vidal, A., Cuenca-Jara, J., Skarmeta, A.F. (2019). IoT for water management: Towards intelligent anomaly detection. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, April 15-18, 2019. https://doi.org/10.1109/WF-IoT.2019.8767190

[37] Yadav, M., Kaushik, A., Garg, R.K., Yadav, M., Chhabra, D., Rohilla, S., Sharma, H. (2022). Enhancing dimensional accuracy of small parts through modelling and parametric optimization of the FDM 3D printing process using GA-ANN. In 2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Pathum Thani, Thailand, Dec. 23-25, 2022. https://doi.org/10.1109/ICCMSO58359.2022.00030

[38] Li, S., Huang, J. (2017). GSPN-based reliability-aware

performance evaluation of IoT services. In 2017 IEEE International Conference on Services Computing (SCC), Honolulu, HI, USA, June 25-30, 2017. https://doi.org/10.1109/SCC.2017.70

[39] Kaushik, A., Gahletia, S., Garg, R.K., Sharma, P., Chhabra, D., Yadav, M. (2022). Advanced 3D body scanning techniques and its clinical applications. In 2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Pathum Thani, Thailand, Dec. 23-25, 2022. https://doi.org/10.1109/ICCMSO58359.2022.00074

[40] Singh, K., Barak, D., Singh, Y. (2023). Reviewing the IoT systems reliability and accuracy. The Pharma Innovation Journal, 12(3): 2775-2780.

[41] Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. Information Systems Frontiers, 18: 665-677. https://doi.org/10.1007/s10796-014-9538-x

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

[43] Sharma, H., Singh, K., Ahmed, E., Patni, J., Singh, Y., Ahlawat, P. (2021). IoT based automatic electric appliances controlling device based on visitor counter. http://doi.org/10.13140/RG.2.2.30825.83043

[44] Yadav, M., Yadav, D., Kumar, S., Chhabra, D. (2021). 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, 11(6): 8258-8287.

[45] Singh, K., Barak, D., Singh, Y. (2021). IoT Chatbot in insurance. International Journal of Engineering, Management, Humanities and Social Sciences Paradigms (IJEMHS), 33(1): 12-16.

[46] Sinche, S., Polo, O., Raposo, D., Femandes, M., Boavida, F., Rodrigues, A., Pereira, V., Silva, J.S. (2018). Assessing redundancy models for IoT reliability. In 2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), pp. 14-15. IEEE. https://doi.org/10.1109/WoWMoM.2018.8449816

[47] Yadav, M., Yadav, D., Garg, R.K., Gupta, R.K., Kumar, S., Chhabra, D. (2021). Modeling and optimization of piezoelectric energy harvesting system under dynamic loading. Advances in Fluid and Thermal Engineering. https://doi.org/10.1007/978-981-16-0159-0_30

[48] Fernandes, J., Raposo, D., Armando, N., Sinche, S., Silva, J.S., Rodrigues, A., Pereira, V., Oliveira, H.G., Macedo, L. Boavida, F. (2020). ISABELA–a socially-aware human-in-the-loop advisor system. Online Social Networks and Media, 16: 100060. https://doi.org/10.1016/j.osnem.2020.100060

[49] Nõmm, S., Bahşi, H. (2018). Unsupervised anomaly based botnet detection in IoT networks. In 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, Dec. 17-20, 2020. https://doi.org/10.1109/ICMLA.2018.00171

[50] Kim, M. (2016). A quality model for evaluating IoT applications. International Journal of Computer and Electrical Engineering, 8(1): 66. https://doi.org/10.17706/ijcee.2016 .8.1.66-76

[51] Safaei, B., Monazzah, A.M.H., Bafroei, M.B., Ejlali, A. (2017). Reliability side-effects in Internet of Things application layer protocols. In 2017 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, Dec. 20-22, 2017. https://doi.org/10.1109/ICSRS.2017.8272822

[52] Lyu, Y., Yin, P. (2020). Internet of Things transmission and network reliability in complex environment. Computer Communications, 150: 757-763. https://doi.org/10.1016/j.comcom.2019.11.054

[53] Li, L., Jin, Z., Li, G., Zheng, L., Wei, Q. (2012). Modeling and analyzing the reliability and cost of service composition in the IoT: A probabilistic approach. In 2012 IEEE 19th International Conference on Web Services, Honolulu, HI, USA, June 24-29, 2012. https://doi.org/10.1109/ICWS.2012.25

[54] Özen, E., Mukul, Taneja, S. (2022). Empirical analysis of the effect of foreign trade in computer and communication services on economic growth in India. Journal of Economics and Business Issues, 2(2): 24-34.

[55] Özen, E., Genc, E., Kaya, Z. (2014). Estimation of the costs of traffic accidents in Turkey: An evaluation in terms of the insurance and financial system. Yaşar Üniversitesi E-Dergisi, 9(33): 5649-5673. https://doi.org/10.19168/jyu.94397

[56] Kumar, P., Taneja, S., Özen, E., Singh, S. (2023). Artificial intelligence and machine learning in insurance: A bibliometric analysis. Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy. https://doi.org/10.1108/S1569-37592023000110A010

[57] Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Eleftherios, T. (2023). Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited, Bingley, UK. https://doi.org/10.1108/S1569-37592023000110A016

[58] Bhatnagar, M., Özen, E., Taneja, S., Grima, S., Rupeika-Apoga, R. (2022). The dynamic connectedness between risk and return in the fintech market of India: Evidence using the GARCH-M approach. Risks, 10(11): 209. https://doi.org/10.3390/risks10110209

[59] Yeşildağ, E., Özen, E., Baykut, E. (2020). An assessment for financial performance of banks listed in borsa istanbul by multiple criteria decision making. Uncertainty and Challenges in Contemporary Economic Behaviour. https://doi.org/10.1108/978-1-80043-095-220201013

[60] Chung, J.W., Roos, A., De Hosson, J.T.M., Van der Giessen, E. (1996). Fracture of disordered three-dimensional spring networks: A computer simulation methodology. Physical Review B, 54(21): 15094. https://doi.org/10.1103/PhysRevB.54.15094

[61] Scapini, Z.E. (2020). A Markov chain approach to model reconstruction. International Journal of Computational Methods and Experimental Measurements, 8(4): 316-325. https://doi.org/10.2495/CMEM-V8-N4-316-325

[62] Sood, K., Dev, M., Singh, K., Singh, Y., Barak, D. (2022). Identification of asymmetric DDoS attacks at layer 7 with idle hyperlink. ECS Transactions, 107(1): 2171.

[63] Barak, D.D., Singh, K., Ahlawat, P., Sharma, H.K. (2020). Real time tracking system: An IoT based application. In 5th International Conference on Next

Generation Computing Technologies (NGCT-2019). Uttarakhand, India, Dec. 20-21, 2019.

[64] Krishnamurthi, R., Kumar, A., Gopinathan, D., Nayyar, A., Qureshi, B. (2020). An overview of IoT sensor data processing, fusion, and analysis techniques. Sensors, 20(21): 6076. https://doi.org/10.3390/s20216076

[65] Ergun, K., Yu, X., Nagesh, N., Cherkasova, L., Mercati, P., Ayoub, R., Rosing, T. (2020). Simulating reliability of IoT networks with RelIoT. In 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), Valencia, Spain, June 29-July 2, 2020. https://doi.org/10.1109/DSN-S50200.2020.00019

[66] Azghiou, K., El Mouhib, M., Koulali, M.A., Benali, A. (2020). An end-to-end reliability framework of the Internet of Things. Sensors, 20(9): 2439. https://doi.org/10.3390/s20092439

[67] Fazio, M., Celesti, A., Ranjan, R., Liu, C., Chen, L., Villari, M. (2016). Open issues in scheduling microservices in the cloud. IEEE Cloud Computing, 3(5): 81-88. https://doi.org/10.1109/MCC.2016.112

NOMENCLATURE

SVM	Support Vector Machine
RTT	Round Trip Time
TCP	Transmission Control Protocol
RBD	Reliability Block Diagram
GPS	Global Positioning System
ORION	Ontario Research and Innovation Optical Network