ISSN 2047-338

Securing Trust in the IoT: An Exploration of Reliability in Connected Systems

Sana Parveen[1], Shazia Saeed[2], M. Junaid Arshad[3]
[1,2,3]Department of Computer Science, University of Engineering and Technology, Lahore
[1]sanaabutt321@gmail.com, [2]shaziasaeed867@gmail.com

***Abstract*– The Internet of Things (IoT) represents a revolutionary paradigm to transform human society into an intelligent, convenient, and efficient entity, offering significant economic and environmental benefits. However, ensuring reliability stands out as a primary challenge that must be effectively addressed to realize the transformative potential of IoT fully. This article adopts a layered approach to the IoT architecture, identifying and examining reliability challenges associated with specific enabling technologies at each layer. Through a systematic synthesis and review of existing literature on IoT reliability, this article categorizes and reflects on reliability models and solutions across four crucial layers: perception, communication, support, and application. Despite the wealth of research conducted in this field, IoT reliability remains in its early stages of exploration. The article highlights challenging research problems and opportunities, shedding light on current underexplored aspects and anticipating future complexities and dynamics in evolving IoT systems.**

***Index Terms*– Reliability, Cloud Computing, Communication Reliability, Internet of Things (IoT) and Perception**

I. INTRODUCTION

COMPUTER technology has experienced an unprecedented expansion within the last century that it means that computing has become a major part of our lives. Computing devices are used to aid in everyday life activities like shopping, banking, and health care. This is accomplished via critical uses of computers in airplane control, military, and nuclear power plant operations to name a few. Computing, which has had such great influence in our society, has therefore required ensuring that these systems will remain reliable. The inventory of smart cities has not remained a future matter with was hundreds of years away but is now a daily reality being driven by IoT devices that are new additions to the current municipal development efforts. The smart infrastructure comprising of smart lightening, intelligent waste management, and efficient public transport is built to sustain the environment by gaining of efficiency, reducing the consumption of energy and improving the overall city live-ability. The Internet of Things (IoT) is an upcoming area within computing that is going through a breakthrough process. Even though this fast progress has been realized, there are some research problems still emerging, like trusting or securing data, interoperability of data, reliability of data delivery, scalability of data, performance, availability, and mobility.

The IoT's responsibility extends to managing devices that may be constrained by nature, such as traffic lights, health systems, and home security. The impact of unreliable IoT infrastructure on decision-making processes, especially in critical scenarios, poses significant challenges. Beyond device and hardware concerns, the reliability of the network layer is also crucial, complicated by the heterogeneous nature of connected devices and wireless data transmission over lossy links. The accuracy of decision-making models and the potentially life-threatening consequences of incorrect decisions heighten the significance of reliability in IoT systems.

Vulnerabilities in IoT devices have become prominent in both consumer and government industries, leading to the issuance of guidelines by the UK government in 2018 for minimum standards in smart-home devices. This underscores the necessity of comprehensively addressing IoT system reliability for the technology to mature fully. Quantifying the reliability of IoT infrastructure and determining which applications can benefit from it are essential steps in ensuring the fitness for purpose of critical IoT infrastructure.

This report presents a comprehensive study of reliability in the context of IoT, starting with an examination of reliability fundamentals in engineering and their application to computing and IoT. It includes an exhaustive literature review, the first of its kind, offering insights into the current state-of-the-art research on IoT reliability.

Significance of Reliability: The thing that can make the Internet of Things (IoT) deployments successful is not much about technical functionality, but reliability. In my opinion, this factor can change how smart device users see technology. Reliability ensures the availability of devices in the continuity of operations, thus performance of IoT is maintained at an optimum level which also lead to a satisfied user. Users are beta-testers for these devices implicitly, leaving them in charge of wide-ranging responsibilities from smart homes to helpful healthcare. The integrity of an IoT system is of paramount significance in the areas with high stakes where failure could

lead to severe consequences for those affected. This sustains the essence of the role of IoT in the scenarios affecting individual welfare and insecurity. Through resolving these issues, tempering the problems, and maintaining the brand image - these reach not only the market expectation but exceed them, as well. It serves as an instrumental factor in raising awareness and encouraging others to onboard IoT technologies, which further increase their chances of being adopted. However, a reliability should not be seen as the technical aspect bringing only the user's trust with a crucial role in a long-run success of IoT integration across our everyday life.

II. RESEARCH OBJECTIVES AND SCOPE

The primary objectives of this research are twofold: this article will be taken to, i) elaborate the crucial role of reliability in the view of the Internet of Things and ii) to observe the significant modification of the trust and confidence of the users in IoT environments. Rather, the study focuses on an analysis of the numerous facets of reliability which exist within distinct layers of the IoT framework, namely perception, communication, support, and application layers. Research which focuses on the problems posed by the technologically enabling aspects at each layer, completes the circle of formulating an informed understanding regarding reliability matters within the IoT ecosystem. In addition to this scope of work, there is also a need to undertake the process of comprehensive and constructive literature synthesis and review which will cover the subject of both IoT reliability. This relates to the probability models and actions for reliability, which are part of this discipline. their key strength, which happens to come from their practical use in real-world scenarios. Even if enough studies already exist, the issues related to IoT reliability are still perceived as immature, thus, this work attempts a systemic study of the current underexplored IoT system patterns along with those of future emerging trends grounded to the complexity and dynamics of the evolving IoT system. this experiment is aimed at enhancing the available existing knowledge by exposing different face of IoT reliability and its effects on system user's trust. Additionally, later part of this section formulates focused objectives and constrains the scope of the review to elaborate a detailed critique of literature on IoT robustness, to elaborate on identified challenges and to recommend exploratory studies.

III. RELIABILITY ON THE INTERNET OF THINGS

Understanding what the Internet of Things (IoT) means is crucial when talking about reliability issues in this field. Sometimes, people do not explain IoT well enough (Atzori et al. 2017). They might say it's about making everyday things connect to the internet, like having your toaster talk to your fridge. While that is true for part of IoT, it does not cover everything. Let us break down IoT into its key parts: sensing, actuating, communication, services, and applications (Rayes and Salam 2016). Think of these as the building blocks. These parts fit into an architecture, like a plan, Sensing and actuating happen at the bottom layer, called the device layer.

Going up, the edge layer helps devices communicate with the application layer. Usually, this communication is done by devices acting like hubs. They collect data from sensors, send it to the cloud, and tell actuators what to do.

Now, if we put all these IoT parts together, we can say IoT is a way of making everything connect and work together. It builds a system for watching and controlling things, and we use this system in different applications to make our daily experiences better (Rayes and Salam 2016).

Device reliability: From a device standpoint in the realm of IoT, the primary challenge lies in the highly constrained nature of sensors and actuators (Al-Fuqaha et al. 2015). These constraints involve limitations in battery life, memory, and computational capacity (Kouicem et al. 2018). Battery concerns are significant, as the application layer often lacks awareness of remaining battery life, making it challenging to predict when a device requires a battery replacement (Shi et al. 2016). The memory and CPU constraints restrict the device's ability to employ complex encryption methods, necessitating reliance on lightweight encryption for data protection (Rayes and Salam 2016; Alaba et al. 2017).

Furthermore, updating firmware for these low powered sensors is impractical due to power limitations, making routine connections to a cloud service for firmware checks unrealistic and potentially leaving devices with outdated firmware, vulnerable to security breaches (Chiang and Zhang 2016; Yaqoob et al. 2017; Allhoff and Henschke 2018).

Devices in IoT, deployed in remote and harsh environments, face environmental challenges such as extreme temperatures, mechanical wear, vibration, and moisture (Rayes and Salam 2016).

Determining the "useful life" of a device becomes crucial, especially in harsh conditions, leading to variances in device lifetime and making system reliability management challenging. A key problem with device reliability is the case of "fail-dirty" occurrence when sensors continue to transmit wrong data after the failure while sensors can radiate high levels of pulse (Karkouch et al. 2016, 2017). This issue is a tricky one since it may not show up as the sensor looks ok, and this may be decisive in the realm of IoT when the wrong readings can lead to a substantial impact, and this can become even more dangerous when actuation is related to the human life.

Communication and network reliability: The issues occurring from the fact of IoT devices being resource constraint, meaning energy depletion, low storage and low computing capability cannot be ignored. The problem of zero monitoring of the batteries levels in IoT applications acquires the status of a well-grounded one as devices are unaware of the residual charge, resulting in the malfunction and operational problems during battery replacement operations, in particular, in physically inaccessible locations. Further, limited in memory and an even smaller sized CPU core, so that they have borderline capacity to integrate anything better than lightweight encryption, hence deciding to rely on the use of light encryption to enhance data security. Along the line, the siting of sensors and actuators in hard environmental conditions with different climates brings additional complexities in the matter related to the term of service of

devices. One of the other problems is the fact that different system environment has different device ages, and hence, the difficulty in system reliability management increases. Another issue which needs attention is around the occurrence of sensor failures, especially the case of "fail-dirty". In such cases, sensors continue to emit erroneous results even after the normal failure. Identifying this issue is a tricky, as it is pretty much okay for a sensor to look fine and have its data right but with the implications of the false readings in the IoT networks being too severe, especially given the fact that human life is risky, the immediate need to divert the faulty sensors is very critical. IoT network mobility implies a few difficulties, such as, global terminal identification conflicts due to the lack of globally unique identifiers for devices across manufacturers does not allow devices tracking, so auditing becomes impossible. The challenge of the traditional Internet Protocol (IP) for IoT is its inefficiency as we see in the loop of IPv4 and its limitations, so we need other protocols like IPv6 and 6LoWPAN. Connection reliability cannot be estimated well neither the IoT devices those coming with different standards and protocols among the IoT devices no quality-of-service guarantee says. The challenges pertaining to noisy signals and their significant variations, and the unreliability in communication over resources limited and intermittently connected IoT networks only exacerbate the issue of making sure that the networks are reliable and secure in the dynamically changing landscape of the Internet of Things.

Application layer reliability: SEE: Abide by this, the application layer behaves without such denials as the network or device layers, while their trustworthiness is related to the ability of these lowers ones to offer these services. Devices can manifest patterns that differ from the established routine of the network and affect the application layer result in a termination of application reliability. That being said, reinforced anomaly detection systems at the application level are vital to identify and rectify errors, particularly the ones with which diverse constrained devices that are transmitting data in the many different formats in an IoT network are being challenged. In addition to non-fixedness of the device layer they operate in, firmware security of the deployed applications is of paramount significance. This research for instance is specified by Moore et al. (2019) showing that unexpected information such as human activity identification is disturbed by an awkward data flow like IoT applications. There may be some classifiers, which have higher chances of making mistakes than the others, and data preprocessing approach also plays role in vulnerability in applications development.

Developers must actively assess and comprehend the reliability of applications hosted in IoT infrastructure to mitigate the risk of critical errors compromising system integrity.

IV. METHODOLOGY

For this study, we adopted a comprehensive literature review method. We found articles, conference papers, and book chapters related to secure data transmission using IEEE Xplore, ScienceDirect, and Google Scholar, which were published in relevant academic databases (Table I). Search words that have been picked, comprise of "IoT", "resource allocation", "latency management", "security", "reliability metrics", and the similar synonyms. "Peer-reviewed" "articles of the past five years were primarily considered as we wished they would have most relevance and application to the current developing technology trends." After gathering relevant literature, we categorized the research into four major areas: resource allocation, latency management, security factors and reliability.

V. RELATED WORK

A) Challenges in IoT Reliability

Hardware Limitations: The issues pertaining to the hardware components of embedded devices encompass performance limitations, the shorter range of data transmission, and the more vulnerable architecture to hardware failures. The reliability and the longevity of IoT devices are thus limited as a result, and this has a practical impact on their overall operation and capability.

Software Complexity: The extensiveness of IoT software, software bugs and vulnerabilities, compatibility challenges from different platforms and devices are the factors that make the complexity of reliability concerns even more adult. Robustness and stability are significant in the expectation of every component's safe delivery in IoT systems.

Interoperability: Inter-operability problems are the essential obstacles an E2E communication and data sharing-wide between all the IoT equipment and standardized systems. Various obstacles, including different versions of communication protocols, data formats, and device standards exist that challenge the IoT interoperability, and its dependability and scalability are affected.

Scalability: IoT systems must deal with growing numbers of connected devices and data volumes as they scale. With that comes another challenge, scalability, which becomes a significant factor. The management of the continuously growing complexity and net traffic together with the assurance of reliability becomes more complicated which leads to all efforts to be made which are aimed at scalable architectures and efficient resource applications.

Security Concerns: IoT systems must cope with a lot of security threats and vulnerabilities what makes them particularly important obstacles to reliability and authenticity of IoT systems. Applications in the smart city may include unauthorized access, data breach and malicious cyberattacks, which pose the key challenge in all three spheres of data confidentiality, integrity, and availability.

B) Opportunities for Improving IoT Reliability

Advanced Sensor Technologies: MEMS sensor and AI powered sensors progress increases the potential of IoT devices for better performance and improved accuracy. Through such technologies, it becomes possible for more accurate data acquisition, actual-time supervision and predictive analytics dashboarding, to name a few, that facilitate and enhance reliability and efficacy.

Table I: Overview of the Literature Survey

Paper Title	Year	Purpose	Research Gap	Problem Statement	Conclusion	Future Work
Enhancing IoT Security: A Review of Current Trends and Future Directions	2022	Review current trends and propose future directions in IoT security	Limited focus on reliability as a cornerstone of IoT trust	Increasing cyber threats and vulnerabilities in IoT ecosystems pose significant security challenges	Collaborative efforts and advanced technologies are essential for mitigating IoT security risks	Empirical studies on IoT reliability, novel privacy approaches, standardized frameworks for certification are essential.
Reliable Internet of Things: Challenges and Future Trends	2021	The paper is designed to emphasize the vital importance of data reliability to the functioning of Internet of Things applications that makes up the beginning of the article and is broadly described in the next parts.	However, despite the advancements not everything is perfect. The gaps are still there from resource allocation, latency, security to the lack of metrics which plead to study to make the IoT operations seamless.	The central problem addressed in this paper is the need for reliable communication in IoT applications. Ensuring the uninterrupted and secure transmission of data between IoT devices is essential for the effective deployment and operation of IoT systems.	this paper underscores the critical importance of reliable communication in IoT applications and highlights the various challenges and limitations currently impeding its realization	Emphasizing the criticality of reliable IoT communication, this paper calls for continued research to address challenges and innovate in resource management, latency reduction, security enhancement, and metric standardization for future IoT advancement.
Reliability of IoT Devices: A Systematic Review	2020	Systematically review the reliability aspects of IoT devices	Limited understanding of reliability factors affecting IoT device performance	Unreliable IoT devices compromise system functionality and user trust	Standardized testing methodologies and quality assurance practices are imperative for improving IoT device reliability	Develop standardized testing, enhance fault tolerance, predictive maintenance to boost IoT reliability across diverse applications.
IoT Security and Privacy: A Review of Current Challenges, Solutions, and Future Directions	2020	Review challenges, solutions, and propose future directions in IoT security and privacy	Insufficient emphasis on the intersection of security, privacy, and reliability in IoT ecosystems	Privacy breaches and security vulnerabilities undermine user trust in IoT systems	Holistic approaches integrating security, privacy, and reliability are essential for ensuring trust in IoT environments	Explore new security techniques, standardize trust evaluation to promote user confidence in IoT environments.
New Frontiers in IoT: Networking, Systems, Reliability, and Security Challenges	2020	The paper intends to highlight the open issues in IoT related to the problems of computer systems, communication, reliability, and security to some extent.	there is a lack of integrated approaches that simultaneously tackle issues such as correlated failures, debugging in production failures, and privacy preserving machine learning techniques to ensure the robustness and trustworthiness of IoT deployments.	The problem statement of the paper is to delineate the open challenges in IoT, aiming to guide research and development efforts toward addressing complexities and constraints inherent in IoT systems.	It endeavors to provide insights into foundational aspects and avenues for addressing these challenges, guiding future research and development efforts in the field.	In the future, it is essential to polish and optimize methodologies for handling correlation problems, for locating and repairing runtime failures and for ensuring reliability, while also building advanced security solutions to reduce risks and maintain data integrity.

Edge Computing: Implementing edge computing architectures helps alleviate the reliability problem due to the data processing is nearer to the source, which means there is less latency, and it is easier to make certain decisions. Edge Computing helps to make the networking of IoT systems even more autonomous and robust, allowing it to function without interruptions in case of connection problems or delays.

Predictive Maintenance: The predictive maintenance systems, which are the bridges between the usage of machine learning algorithms and predictive analytics, provide chances to foresee and eliminate potential failures in the pre-planning stage.

Blockchain Technology: Beyond the promise, the Blockchain technology has shown itself to be superior in terms of integrity and resourcefulness for the IoT systems by providing viable data storage, a peer-to-peer agreement mechanism, and records on transactions. Through combining blockchain with data integrity and authentication for IoT implementations, risks arising from the security can be circumvented, and trust will also be elevated.

Standardization and Best Practices: Unified protocols, interoperability standards and optimal design guidelines are fundamental in the establishment of a good system that cater for reliability and scalability. Create one cohesive approach that positions industry on the path of interoperability as well as smooth integration and raises the bar of reliance on the IoT solution.

VI. CONCLUSION

In 2024, addressing reliability and resilience challenges will remain critical as IoT applications expand across industries, from healthcare to smart cities, where uninterrupted operation and data integrity are imperative for success. To add, IoT is an incredible field to be working in, its system, networks, reliability, security, or privacy all the areas provide a lot to work in. A surge of reputable as well as groundbreaking technical challenges is foreseen through the same time duration together with a growing atmosphere of convincing solutions, with many more to come.

REFERENCES

[1]. Petrakieva, S., Garasym, O., & Taralova, I. (2014). http://ieeexplore. ieee. org/stamp/stamp. jsp? tp= &arnumber= 7038771.

[2]. Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W. S. (2024). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. *Transactions on Emerging Telecommunications Technologies*, *35*(4), e4329.

[3]. 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.

[4]. Khan, M. Z., Alhazmi, O. H., Javed, M. A., Ghandorh, H., & Aloufi, K. S. (2021). Reliable Internet of Things: Challenges and future trends. *Electronics*, *10*(19), 2377.

[5]. Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University Computer and Information Sciences*, *30*(3), 291-319.

[6]. Xing, L. (2020). Reliability in Internet of Things: Current status and future perspectives. *IEEE Internet of Things Journal*, *7*(8), 6704-6721.

[7]. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28.

[8]. Pokorni, S. J. (2019). Reliability and availability of the Internet of things. *Vojnotehnicki glasnik/Military Technical Courier*, *67*(3), 588-600.

[9]. 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.

[10]. Alam, T. (2018). A reliable communication framework and its use in internet of things (IoT). *CSEIT1835111| Received*, *10*, 450-456.

[11]. Zin, T. T., Tin, P., & Hama, H. (2016, October). Reliability and availability measures for Internet of Things consumer world perspectives. In *2016 IEEE 5th Global Conference on Consumer Electronics* (pp. 1-2). IEEE.

[12]. Mavrogiorgou, A., Kiourtis, A., Symvoulidis, C., & Kyriazis, D. (2018, October). Capturing the reliability of unknown devices in the IoT world. In *2018 Fifth International Conference on Internet of Things: Systems, Management and Security* (pp. 62-69). IEEE.

[13]. Kim, M. (2016). A quality model for evaluating IoT applications. *International Journal of Computer and Electrical Engineering*, *8*(1), 66.

[14]. Saini, N. K. (2016, January). Trust factor and reliability-over-a-period-of-time as key differentiators in IoT enabled services. In *2016 International Conference on Internet of Things and Applications (IOTA)* (pp. 411-414). IEEE.

[15]. Li, F., Nastic, S., & Dustdar, S. (2012, December). Data quality observation in pervasive environments. In *2012 IEEE 15th International Conference on Computational Science and Engineering* (pp. 602-609). IEEE.

[16]. Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., & Coen-Porisini, A. (2016). A secure and qualityaware prototypical architecture for the Internet of Things. *Information Systems*, *58*, 43-55.

[17]. 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.

[18]. Rizzardi, A., Miorandi, D., Sicari, S., Cappiello, C., & Coen-Porisini, A. (2016). Networked smart

[19]. objects: Moving data processing closer to the source. In *Internet of Things. IoT Infrastructures: Second International Summit, IoT 360° 2015, Rome, Italy, October 27-29, 2015, Revised Selected Papers, Part II* (pp. 28-35). Springer International Publishing.

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

[21]. Kamyod, C. (2018, February). End-to-end reliability analysis of an IoT based smart agriculture.

[22]. In *2018 International Conference on Digital Arts, Media and Technology (ICDAMT)* (pp. 258-261). IEEE.

[23]. Brogi, A., & Forti, S. (2017). QoS-aware deployment of IoT applications through the fog. *IEEE internet of Things Journal*, *4*(5), 1185-1192.

[24]. Al-Masri, E. (2018, October). QoS-aware IIoT microservices architecture. In *2018 IEEE International Conference on Industrial Internet (ICII)* (pp. 171-172). IEEE.

[25]. Li, S., & Huang, J. (2017, June). GSPN-based reliability-aware performance evaluation of IoT services. In *2017 IEEE International Conference on Services Computing (SCC)* (pp. 483-486). IEEE.

[26]. Sinche, S., Polo, O., Raposo, D., Femandes, M., Boavida, F., Rodrigues, A., ... & Silva, J. S. (2018, June). 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.

[27]. Alam, T. (2018). A reliable communication framework and its use in internet of things (IoT). *CSEIT1835111| Received*, *10*, 450-456.

[28]. Behera, R. K., Reddy, K. H. K., & Roy, D. S. (2015, September). Reliability modelling of service-oriented Internet of Things. In *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)* (pp. 1-6). IEEE.

[29]. Kharchenko, V., Kolisnyk, M., Piskachova, I., & Bardis, N. (2016, August). Reliability and security issues for IoT-based smart business center: architecture and Markov model. In *2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)* (pp. 313-318). IEEE.