International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 13 Issue 6 ǁ June 2025 ǁ PP. 48-57

Certain Investigations on System Level Challenges in Internet of Things

[1]Manikandan.S, [2]Dr. Marikkannan.M
[1]*M.E. Computer Science and Engineering (PG Scholar), Department of CSE, Government College of Engineering, Erode, TN.*
[2]*Assistant Professor (Senior), Department of CSE, Government College of Engineering, Erode, TN.*

Abstract
The proliferation of Internet of Things (IoT) devices has introduced significant challenges in scalability, interoperability, security, and network reliability. Traditional operating systems and scheduling algorithms often fall short in meeting the real-time demands of IoT applications, leading to issues like indefinite delays for low-priority tasks and non-deterministic I/O event handling. The absence of unified standards exacerbates interoperability problems across diverse platforms and architectures. Security concerns are paramount, with threats such as radio jamming, unauthorized access, and data breaches prevalent due to the heterogeneous and resource-constrained nature of IoT networks. While blockchain offers decentralized security solutions, it introduces challenges related to energy consumption and computational overhead. Emerging technologies like deep learning and reinforcement learning show promise in enhancing intrusion detection systems and adapting security measures in real-time. Scalability remains a pressing issue, especially as centralized cloud frameworks prove inefficient for time-sensitive applications, prompting a shift towards fog computing to leverage edge resources. Network survivability is threatened by cascading failures, particularly when critical components like base stations are compromised. Strategies such as deploying additional gateways and optimizing their placement have been explored to bolster network resilience. In the realm of Industrial IoT (IIoT), knowledge-based fault diagnosis using ontologies and inductive reasoning is gaining traction, though challenges persist in distributed systems due to knowledge base isolation and scalability concerns. Addressing these multifaceted challenges necessitates the development of adaptive, secure, and interoperable network management solutions tailored to the dynamic and diverse IoT landscape.

Keywords: *IoT Architectures, Smart Applications, IIoT, Security, Privacy, Trust issues.*

Date of Submission: 24-05-2025 Date of acceptance: 04-06-2025

I.INTRODUCTION

The Internet of Things (IoT) connects physical and virtual devices to enable intelligent services. However, its rapid growth raises significant concerns regarding security, privacy, and trust across all layers - physical, network, and application - requiring robust solutions to ensure safe, reliable operation. Highlights IoT as the third wave of the internet, enabling smart environments through connected devices. It emphasizes IoT's applications, intelligence, and real-world impact, while also addressing challenges like limited computation, energy, storage, and security constraints [5]. It connects everyday physical devices intelligently to enhance daily life. However, managing heterogeneous, resource-constrained IoT networks poses challenges like congestion and failures. In [14], reviews existing low-power IoT network management solutions - protocols, cloud, Software Defined Networking (SDN), semantic, and ML-based - highlighting their limitations, requirements, and open research challenges. Highlights IoT's evolution from simple data sharing to real-time data collection, analysis, and control. It emphasizes IoT's wide applications, massive growth, and the complexity of its ecosystem involving end-nodes, edge, fog, cloudlets, and cloud. Challenges include energy efficiency, heterogeneity, interoperability, and security, requiring tailored system-level solutions beyond traditional approaches [1].

Cascading failures in IoT systems, emphasizing their causes, modeling approaches, and mitigation strategies. It distinguishes between reliability and resilience, explores existing research gaps, and highlights the importance of enhancing IoT robustness against cascading failures [2]. Cascade failure model tailored for IoT networks, considering node roles and routing protocols. It introduces load redistribution schemes and gateway placement strategies to enhance IoT reliability against cascading failures triggered by overload and dynamic topology changes [4]. IoT networks face failures from attacks and malfunctions; cascading failures from load redistribution can collapse entire systems, making survivability through routing and topology resilience critically important [3]. IoT systems are increasingly used in safety and mission-critical applications, where reliability is essential. However, IoT devices are prone to failures due to faults, outages, or data loss, leading to severe

consequences. [11] surveys IoT reliability modeling, analysis, and design across a four-layer architecture. It highlights challenges, solution methods, and future directions, emphasizing reliability's critical role in mission - and safety-critical applications across diverse IoT domains and technologies.

IIoT systems face essential risks of fault due to interconnected components and human interaction. Knowledge-based fault diagnosis using ontologies and reasoning (deductive/inductive) enhances system reliability. Distributed and scalable diagnosis methods are essential to address privacy, interoperability, and computational challenges [10].

II.BACKGROUND SURVEY

2.1 Related Works and Contribution

In [1], provides an overview of the current advancements in the IoT and its applications. It outlines the existing architecture of IoT systems, focusing on their contemporary status and development. Addresses the challenges and solutions related to creating real-time, energy-efficient, scalable, reliable, and secure IoT applications. It highlights the importance of different communication standards in IoT and the challenges of ensuring interoperability between them. [2] focuses on the modeling and reliability analysis of cascading failures in IoT systems, along with strategies for improving resilience. And it systematically reviews how cascading failures occur in IoT systems, exploring the methodologies for modeling these failures and analyzing their impact.

In [3], presents a realistic cascading model for IoT systems, considering the real-world characteristics like data aggregation and link heterogeneity. It introduces a model based on the layered architecture of IoT systems, where cascading failures are triggered by overload events occurring in relay nodes, base stations, and communication links. To improve the network survivability of IoT systems, the paper proposes a load-oriented layout scheme for base stations. This scheme aims to optimize network structure and mitigate cascading failures. Extensive simulations were conducted to verify the soundness of the cascading model and the effectiveness of the proposed layout scheme. The findings include Tolerance parameter space, Base station removal, Increasing the number of base stations.

Focuses on addressing cascade failures in IoT networks, a critical issue limiting their widespread application. It introduces a new metric to characterize the cascade process in IoT networks. This metric, called IoT-oriented router betweenness, helps assess how network nodes (routers) contribute to the cascade failures [4]. In [5], covers the historical development, market growth, and technologies behind IoT, while also comparing it to the general Internet and showcasing its role in creating smart applications across industries.

In [6], focuses on the application of Artificial Intelligence (AI) and Machine Learning (ML) in solving complex, high-dimensional, and dynamic problems within multi-RAT (Radio Access Technology) IoT networks. It explores how AI and ML techniques can be used to manage the complexities of multi-RAT IoT networks, particularly focusing on inter-layer dependencies and cross-layer design. [7] review delves into the critical areas of IoT security, privacy, and trust using a 3-layer IoT architecture. It introduces the basic principles and significance of security, privacy, and trust in the IoT environment. It examines the security needs within IoT architectures, highlighting the common challenges that arise in ensuring the protection of IoT systems.

[8] provides a current analysis of IoT applications in agriculture. In that explores the technological advancements that support the deployment of IoT in agriculture, focusing on innovations that make IoT applications feasible. It examines how IoT is being applied in agriculture, particularly in addressing various challenges in the sector, such as improving crop yield, monitoring soil health, and optimizing water usage. Highlights the role of machine learning models in enhancing IoT applications, enabling smarter, data-driven decisions in agriculture. [9] focuses on the concept of smart cities. It provides a brief introduction to the concept of smart cities, highlighting their importance and development. It explores the key characteristics and features that define smart cities, including their infrastructure and technological components. It addresses the generic architecture of smart cities and provides examples of real-world implementations, showcasing how these cities are being developed globally. It identifies various challenges in the development of smart cities, such as the use of big data and analytics, and outlines the opportunities these challenges present for improvement. It emphasizes the potential for developing better applications and solutions by leveraging the technologies associated with smart cities.

[10] focuses on fault diagnosis in Industrial Internet of Things (IIoT) systems, which are composed of smart devices like sensors, actuators, and controllers to enable efficient industrial operations. It explores both model-based and data-driven approaches for fault detection in IIoT systems. It emphasizes the importance of designing physical models, signal patterns, and machine learning algorithms that effectively identify and isolate system faults. As IIoT systems grow in scale and connectivity, their complexity increases exponentially, making fault diagnosis more difficult. It highlights how the increasing interconnection of devices can complicate traditional fault detection methods. It argues that knowledge-based approaches are more effective than plain model-based or data-driven methods for diagnosing faults in modern IIoT systems. The review provides insights into the construction of knowledge bases via ontologies and the role of reasoning in improving fault diagnosis in

IIoT environments.

In [11], addresses the critical issue of reliability in the IoT, a key factor for the successful transformation of society toward a more intelligent, convenient, and efficient future. It explores the reliability challenges at each of the four layers of the IoT architecture: perception, communication, support, and application. It provides a systematic synthesis and review of existing literature on IoT reliability, presenting reliability models and solutions at each layer. It classifies the various approaches and methods proposed to improve reliability in IoT systems. [13] addresses the importance of reliability and fault tolerance in the rapidly growing IoT applications and systems. It proposes a model-based design approach for IoT systems, where formal models are used to analyze failure-related behaviors early in the development process. It presents a formal model of IoT architectures that takes failure-related aspects into account. This model helps designers understand potential points of failure and their impact on the system's overall reliability. The formal model allows designers to perform reliability analysis using Statistical Model Checking (SMC) and run-time simulations. In [14], offers a thorough analysis of IoT network management, focusing on solutions for low-power IoT networks, and highlights the remaining challenges in ensuring efficient and reliable performance in these networks.

2.2 Research Analysis

To guide researchers, particularly those newly exploring the IoT field, a set of research questions has been formulated. By conducting an in-depth analysis of IoT's evolution over the past decade, these questions aim to direct attention to key areas requiring further investigation.

RQ.1 What are the current advancements in the IoT?
RQ.2 What are the principles and significance of security, privacy, and trust in IoT?
RQ.3 What are the smart applications and automation technologies in IoT?
RQ.4 What are the limitations and challenges of current IoT research?
RQ.5 What are the important future research directions in IoT?

2.3 Motivations

The IoT has emerged as a critical component of the modern technological revolution, particularly in domains such as smart automation, industrial automation, healthcare, and beyond. As IoT continues to drive transformative changes across various sectors, it simultaneously introduces a range of challenges, failures, and security concerns that must be addressed. In response to these developments, this review formulates key research analysis and examines a broad spectrum of references, with particular emphasis on IoT's rapid growth over the past decade, its applications in smart environments, agriculture, big data, healthcare, and Industrial IoT (IIoT). This paper explores critical issues related to IoT architectures, security and trust mechanisms, scalability, interoperability, Quality of Service (QoS), resilience, network management, device management, among others. Ultimately, this review provides a comprehensive summary of the current trends, identifies major challenges, and outlines promising future directions in the field of IoT.

III.OVERVIEW OF IoT

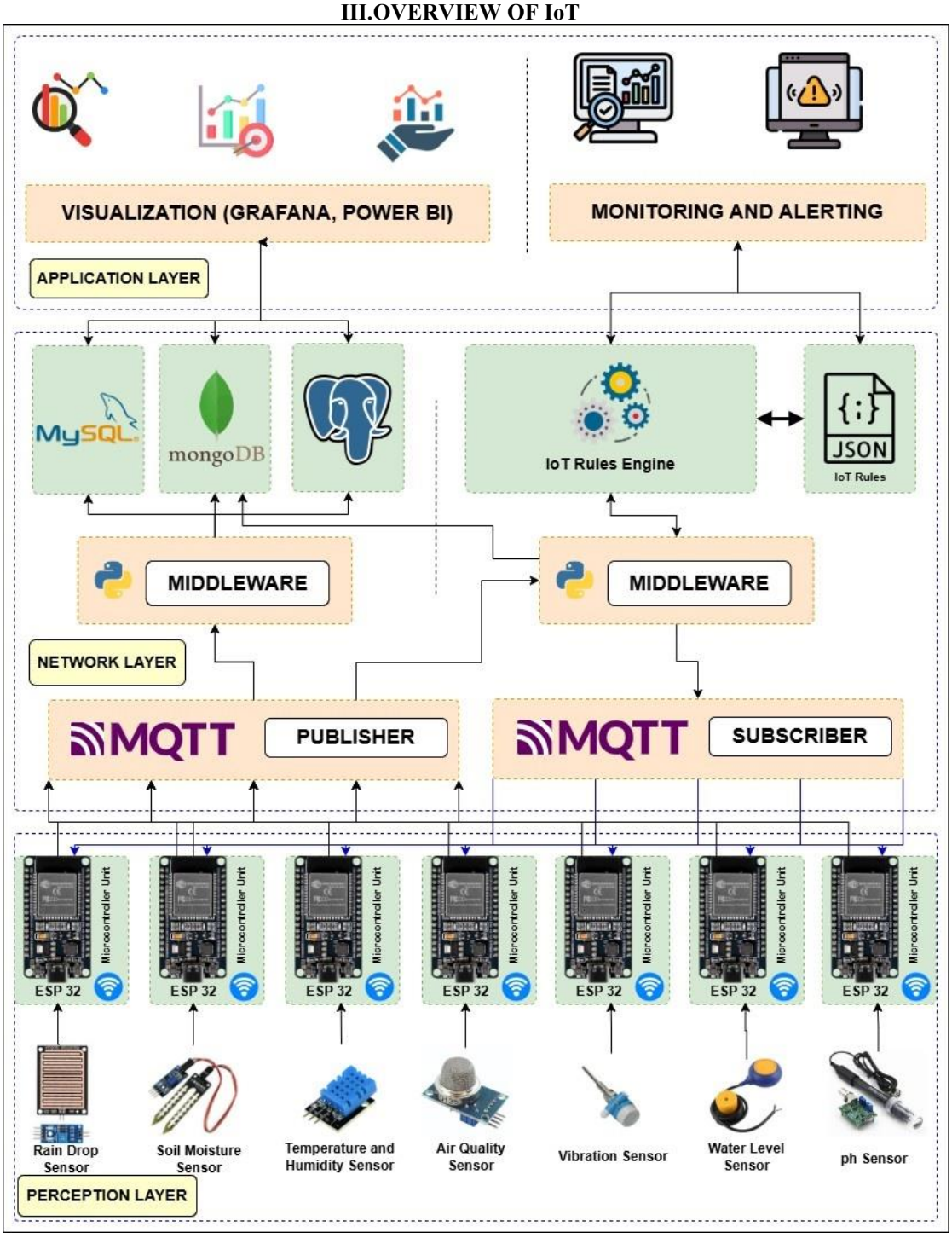

Figure1: Three Layered Architecture

The IoT represents a transformative shift in technology, integrating physical objects with the digital world through network connectivity. By enabling everyday devices such as sensors, actuators, appliances, and industrial machines to communicate intelligently, IoT has revolutionized areas like smart homes, healthcare, agriculture, transportation, and industrial automation. Its primary goal is to enhance convenience, productivity, and efficiency in daily life and industrial processes. With advances in low-power devices, communication technologies, and lightweight protocols, IoT has seen widespread adoption. IoT systems typically rely on a layered architecture involving end nodes, edge computing, fog nodes, cloudlets, and cloud infrastructure, allowing for real-time data processing and analysis. However, the large-scale, heterogeneous, and resource-constrained nature of IoT deployments introduces significant challenges, including issues related to network congestion, device failures, energy efficiency, resilience, scalability, data integrity, interoperability, and data management. Security,

privacy, and trust have become fundamental concerns in IoT systems, given the sensitive nature of the data being collected and shared across diverse networks. IoT devices are vulnerable across the physical, network, and application layers, making it critical to design robust security frameworks tailored to the specific constraints of IoT environments.

Despite its rapid development, IoT research faces limitations such as resource constraints, lack of unified standards, data privacy risks, and the need for more efficient management of large-scale deployments. Future research directions emphasize enhancing system scalability, developing lightweight security protocols, achieving better interoperability among diverse devices, optimizing QoS, and ensuring sustainable energy usage. As IoT continues to grow, addressing these challenges will be crucial to fully realize its potential across industries and society [1-14].

The Figure1 represents the architecture for real-time monitoring of IoT devices is structured into three main layers: Perception Layer, Network Layer, and Application Layer. At the Perception Layer, various types of sensors are connected to an ESP32 microcontroller. These sensors collect physical parameters from the environment, and the microcontroller aggregates the data. The ESP32 then transmits the collected sensor data to the cloud using the Message Queuing Telemetry Transport (MQTT) protocol. The Network Layer handles the data reception and processing. A subscriber service, operating as a system service on the server, listens for incoming MQTT messages and stores the raw sensor data into a database, such as MySQL, MongoDB, or PostgreSQL, depending on system requirements. Simultaneously, a middleware handler processes the received device health status and sensor data. This handler cross-verifies the incoming data against pre-defined IoT rule sets to assess data integrity and device health conditions. The results of this analysis are also stored in the database for further evaluation.

At the Application Layer, the stored sensor data is forwarded to visualization platforms such as Grafana or Power BI for real-time dashboards and analytics. Meanwhile, the device health information is used to update network monitoring dashboards, which provide alerts and system status updates. If any anomalies or rule violations are detected, the system triggers identification and rectification processes. AI and ML algorithms will be integrated to enhance the anomaly detection, fault identification, and predictive maintenance capabilities of the system. This layered approach ensures efficient data acquisition, reliable monitoring, timely alerting, and intelligent decision-making for real-time IoT device management.

IV.EMERGING IoT TECHNOLOGIES

The Figure2 represents various emerging technologies that are transforming and enhancing the IoT ecosystem. In this paper, these technologies are discussed in detail to highlight their roles and potential in addressing the challenges of scalability, security, real-time performance, and interoperability within IoT systems.

4.1 Smart Home

Smart homes aim to enhance the quality of life by integrating IoT technologies across various domains such as home automation, air quality monitoring, healthcare, surveillance, and smart gardening. These systems allow remote control and monitoring of appliances and health, improve safety through real-time surveillance, and promote efficient energy use. Despite their advantages, smart homes face challenges such as device heterogeneity, privacy concerns due to continuous data collection, and cybersecurity risks from device hacking. Effective communication protocols like MQTT and platforms such as Arduino and Raspberry Pi enable smart interactions and control, making smart homes more secure, responsive, and energy-efficient [1, 5].

4.2 Smart Agriculture

Smart agriculture leverages IoT, sensors, and cloud computing to optimize farming through precision agriculture, crop health monitoring, smart greenhouses, and livestock tracking. It enhances productivity, reduces resource waste, and supports sustainable practices. Technologies like drones, deep learning, and automation enable real-time data analysis, improving crop yield, animal health, and environmental management for efficient, data-driven farm operations [1, 5].

4.3 Smart Healthcare

Smart health integrates IoT, wearable sensors, and real-time monitoring to enhance healthcare delivery, reduce costs, and improve quality of life for humans and pets. It enables early diagnostics, chronic disease tracking, fitness monitoring, and emergency care using Global Positioning System (GPS) and telehealth. Key challenges include real-time data processing, device interoperability, energy-efficient algorithms, and maintaining privacy. Smart health transforms clinic-centric care into patient-centric, data-driven healthcare for timely and effective treatment [1].

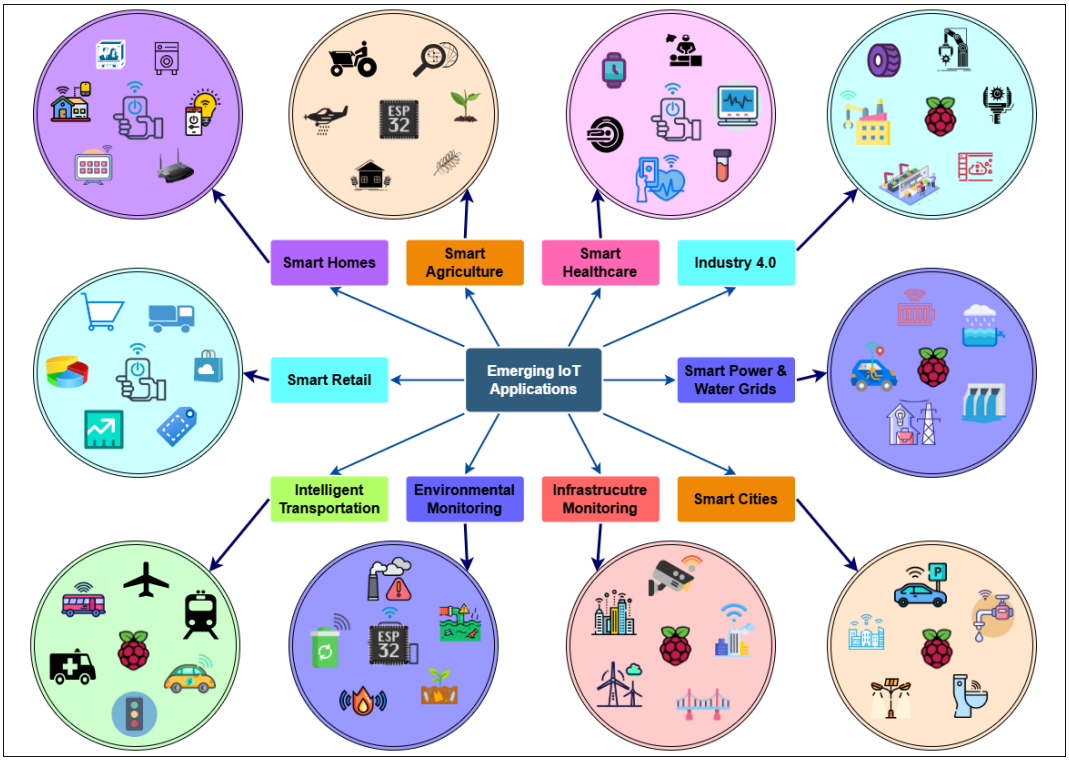

Figure2: Emerging IoT Applications

4.4 Smart Industry 4.0

Industry 4.0, also known as Industrial IoT, enhances manufacturing efficiency using real-time data, automation, and connectivity. It offers benefits like shorter development cycles, better resource use, and improved decision-making. Key areas include plant safety, product monitoring, supply chain management, and quality control. Future Industry 5.0 emphasizes human-machine collaboration, requiring scalable device management, robust security, and intelligent algorithms for safe, adaptive, and efficient operations [1].

4.5 Smart Cities

Smart cities integrate IoT technologies to enhance infrastructure, governance, safety, and quality of life. Key features include smart infrastructure, e-governance, surveillance, and community services like energy, water, and waste management. Real-time data, automation, and self-learning systems improve urban efficiency, decision-making, and sustainability. Smart cities aim to address urban challenges through intelligent solutions for better connectivity, resource management, and citizen well-being [1, 5].

4.6 Infrastructure Monitoring

Infrastructure monitoring uses IoT to track real-time conditions of civil structures, pipelines, aircraft, and military bases, enhancing safety and efficiency. Smart sensors detect damage, cracks, or leaks, enabling timely interventions. Key technologies include deep learning, data fusion, autonomous robots, and secure device management. These systems ensure operational reliability, environmental protection, and effective disaster response while requiring robust connectivity and privacy safeguards [1].

4.7 Environmental Monitoring

Urbanization leads to environmental issues like pollution and natural disasters. IoT helps monitor air and water quality, detect forest fires, manage disasters, and improve water sanitation. Challenges include large, heterogeneous data, sensor durability, and security. Intelligent, lightweight algorithms are essential for accurate, efficient environmental monitoring and timely decision-making [1].

4.8 Intelligent Transportation

Intelligent Transportation Systems (ITS) use IoT for traffic flow control, traveler information, freight management, and vehicle-to-vehicle communication. IoT enhances transportation efficiency, safety, and eco-friendliness through real-time data and adaptive systems. However, challenges like data accuracy, high mobility, privacy, security, and legal concerns must be addressed for effective and secure smart transportation solutions [1, 5].

4.9 Smart Power & Water Grids

Smart power and water grids use sensors and control devices to monitor and manage distribution, improving efficiency and reducing costs. Power grids track load balancing, energy loss, and metering, while water grids monitor parameters like pressure and leakage. Smart metering enhances operational efficiency. Future integration of power and water grids, along with predictive algorithms and sensor fusion techniques, will optimize resource management and consumption [1].

4.10 Smart Retail

Smart retail enhances customer experience using Radio-Frequency Identification (RFID), augmented reality, and communication technologies. It features sensor-based stock tracking, automated checkouts, and recommender systems. Future advancements include Virtual Reality (VR), Augmented Reality (AR), and intelligent robots for virtual trials and personalized shopping. However, these technologies raise privacy and security concerns, necessitating efficient algorithms to analyze customer data and moods [1].

V.RESEARCH CHALLENGES

The Figure3 illustrates the key challenges encountered in the development, deployment, and operation of Internet of Things (IoT) systems. In this paper, these challenges are examined comprehensively to emphasize the limitations and constraints currently affecting the growth and efficiency of IoT technologies.

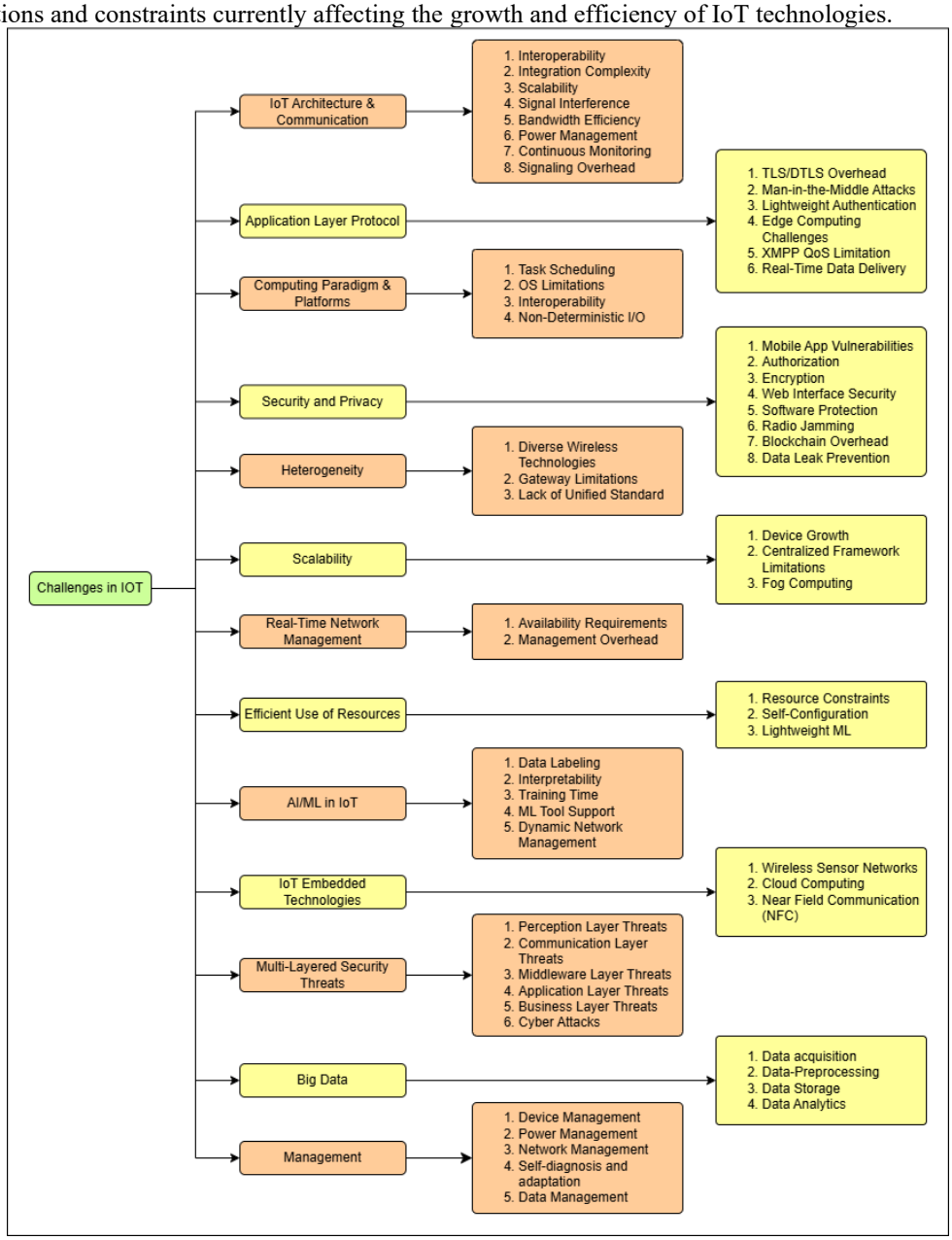

Figure3: Challenges in IoT

5.1 IoT Architecture & Communication

In [1], highlights the lack of interoperability among various computing architectures and platforms, which complicates the integration of multiple IoT applications. Integration challenges arise due to diverse services, protocols, and file formats. Additionally, developing scalable architectures that support mobility remains a significant issue. Interference from the shared 2.4GHz band used by WiFi and Thread increases signal noise and weakens strength. A constant internet connection and open ports are required for global data sharing. Efficient bandwidth usage is crucial, yet current communication technologies like WiFi lack power management. Continuous device monitoring is difficult, and high signaling overhead in 5G networks raises energy consumption. knowledge-based fault diagnosis for IIoT systems, emphasizing its advantages over model-based and data-driven methods. By using ontologies, knowledge-based approaches improve reasoning and support non-expert users in diagnosing faults [10]. the growing concern of network survivability against cascading failures in IoT systems by proposing a realistic cascading failure model based on the layered IoT architecture. A load-oriented layout strategy for base stations is introduced to enhance survivability [3]. Threats are categorized across various layers: perception, communication, middleware, application, and business. Additionally, broader cyberattacks pose risks at every layer, demanding comprehensive, multi-tiered security approaches [8].

5.2 Network & Application Layer Protocol

Security protocols like Transport Layer Security (TLS)/ Datagram Transport Layer Security (DTLS) introduce latency and consume resources due to expensive handshakes. These protocols are also vulnerable to man-in-the-middle attacks, highlighting the need for lightweight, strong authentication. Challenges include data management during the shift from cloud to edge, validation/testing, and addressing privacy concerns such as anonymous communication. Extensible Messaging and Presence Protocol (XMPP) lacks QoS support, doesn't allow high-resolution media sharing, and needs improvements in priority-based data delivery for real-time applications [1]. Local Routing Mode (LRM) is more reliable against cascade failures, requiring fewer capacity resources and experiencing less damage. Increasing the number of gateways enhances network reliability, though the benefit diminishes with each added gateway. Notably, adding gateways improves both cascade resistance and network topology robustness more effectively than just expanding capacity, with the High Degree Placement (HDP) gateway placement strategy outperforming others [4].

5.3 Computing Paradigm

In [1], Issues in IoT computing paradigms include difficulties in efficient resource usage, integration of machine learning, and the need for lightweight computation models. Current paradigms struggle with mobility support, real-time responsiveness, and scalability.

5.4 Security and Privacy

Most IoT applications are controlled via mobile apps, making mobile application security a critical concern. Key issues include authorization, privacy, encryption, securing web interfaces, and software protection within IoT middleware. Radio jamming poses a major threat since most IoT communications rely on wireless standards, while low-power networks struggle with robust security due to resource constraints [1]. Secure network management is essential to prevent data leaks, but limited resources make implementing strong protections challenging. Open ports, necessary for global data sharing, expose devices to serious attacks such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), and code injection [1 , 14]. Real-time communication demands secure device authentication to maintain network reliability [5]. Blockchain offers decentralized security but leads to high energy consumption, storage, and computation overheads. Deep Learning improves Intrusion Detection Systems (IDS) by enabling proactive threat identification, but existing security solutions are often inadequate for the diverse IoT ecosystem. Device heterogeneity and dynamic behavior introduce trust issues, and adaptive security measures, possibly using Reinforcement Learning (RL), are needed. Privacy remains a major concern across IoT domains [7]. In agriculture, multi-layered IoT setups face unique vulnerabilities in data handling and are further complicated by the physical environment's exposure to animals, equipment, and workers. Therefore, context-aware, environment-specific security strategies are essential [8].

5.5 IoT Platforms

Real-time applications face challenges because high-priority tasks may miss deadlines, and low-priority tasks could wait indefinitely. Traditional OS scheduling algorithms are unsuitable for real-time needs, and interoperability issues arise from the wide variety of operating systems, data structures, programming languages, protocols, and IoT architectures. Scheduling for I/O events often lacks determinism, further complicating real-time performance [1]. The lack of unified IoT standards has resulted in non-interoperable architectures, making multi-application integration difficult due to differences in services, protocols, and file formats. Additionally, real-world testbeds like Secure Communication based on Quantum Cryptography (SECOQC) have shown that

even with encryption and Quantum Key Distribution (QKD), data transmission capacities remain limited. Seamless interoperability among platforms such as Azure and IBM IoT is essential, highlighting the need to develop unified, interoperable architectures that support integration across diverse computing environments [5 , 14].

5.6 Efficient use of Resources

Embedded IoT devices face resource constraints in battery, memory, and processing. Ensuring good performance requires self-configuration to handle mobility and failure. ML can aid in management but demands heavy computational/storage resources. Lightweight ML-based frameworks are needed to prevent overloading networks or devices [14].

5.7 Scalability

Scalability is a crucial requirement due to the rapid expansion of IoT devices, yet many current low-power network management solutions struggle to scale effectively. Centralized, cloud-based frameworks are often inefficient for time-sensitive applications such as telemedicine, making fog computing a promising alternative by integrating cloud and edge resources to enhance and accelerate network reconfiguration [14]. Developing architectures that support both scalability and mobility remains a significant challenge, particularly in remote or resource-constrained environments where continuous monitoring is difficult [1]. As millions of devices connect to IoT networks, maintaining consistent, efficient security measures becomes increasingly complex, emphasizing the urgent need for scalable, adaptive management approaches in future research.

5.8 Heterogeneity

IoT networks are becoming increasingly heterogeneous due to the diversity of wireless technologies, with standards like ZigBee, Bluetooth (BLE), NB-IoT, and ISA100.11a facilitating IPv6-based communication [14]. Gateways help bridge IP and non-IP devices through cloud, SDN, or semantic-based frameworks, but current gateways often lack strong Quality of Service support. Managing heterogeneous networks with improved QoS remains a key challenge, highlighting the need for a unified IoT management architecture [6, 7].

5.9 Wireless Sensor Networks

In [5], Efficient and secure data access is critical in Wireless Sensor Networks (WSNs), especially in real-time, high-demand scenarios like battlefields, where authentication mechanisms are essential to ensure that only authorized nodes can access data. WSNs operate in self-organized environments, adding complexity to communication and requiring robust protocols for reliable data management. Real-time communication depends on device authentication to maintain network security and reliability. Protecting sensitive sensor data is crucial, as any alteration can have serious consequences. IoT systems, inheriting features from WSNs and the traditional internet, combine multi-hop communication, scalability, battery constraints, and global access into a more integrated and intelligent framework. [5] Near Field Communication (NFC) is vulnerable to packet loss, cloning, and man-in-the-middle attacks. Security in tag-reader authentication is still weak, and NFC systems struggle with power, processing, and storage limitations. A secure and universal NFC authentication system has yet to be developed.

5.10 Cloud Computing & Big Data Analysis

In [5], Cloud computing addresses the diverse storage and computing needs of individuals and organizations, enabling cost-effective processing of large data volumes from humans, IoT devices, and other sources. It offers high performance, accessibility, and flexibility, making it ideal for various applications. Despite advances, IoT devices still struggle with limited storage and connectivity. Big Data in Smart Cities faces challenges such as data volume, velocity, quality, privacy, and integration, with traditional methods insufficient for dynamic environments. Future research should focus on scalable, secure frameworks for real-time processing, advanced visualization, and citizen-centric designs to ensure high data quality and actionable insights for sustainable urban development [9].

5.11 Management

The integration of numerous devices in Industry 4.0 necessitates robust device and data management to tackle challenges like heterogeneous hardware, frequent updates, and dynamic topologies. Standards such as International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC), Joint Technical Committee (JTC) 1/ Working Group (WG) 9 and Open Mobile Alliance (OMA) protocols help address these issues, focusing on device management including monitoring, diagnostics, updates, and configuration. Data management involves tools like NoSQL databases, Apache Spark, and time-series analytics for efficient data collection, storage, processing, and visualization. Self-diagnosis and machine learning techniques enable fault

detection and system adaptation. In IoT applications like smart healthcare, real-time network management is critical but challenging due to limited resources in low-power IoT networks. Research highlights the need for adaptive, lightweight management techniques to improve performance, prevent data leaks, and ensure secure, efficient real-time network operations [1, 6].

VI.CONCLUSION AND FUTURE DIRECTION

The rapid evolution of the Internet of Things has brought unprecedented opportunities alongside complex challenges in scalability, interoperability, security, reliability, resilience, device management, and network management. This comprehensive analysis highlights that existing architectures, protocols, and management strategies are often inadequate for the diverse and dynamic nature of modern IoT systems. Key issues such as real-time data handling, heterogeneous device integration, limited resources, and vulnerability to cascading failures and security threats remain major barriers to efficient deployment. Emerging technologies like fog computing, reinforcement learning, deep learning, and knowledge-based fault diagnosis offer promising directions to address these limitations. Additionally, the integration of scalable and adaptive solutions, along with optimized gateway and base station deployment, can significantly enhance system resilience and performance. Future research would focus on developing heterogeneity, secure, integrity, availability, resilient, improving fault diagnosis using AI and ontologies. The resource management, and energy-efficient frameworks that support real-time, large-scale, and distributed IoT environments which ensure seamless functionality across the industries.

REFERENCES

[1]. S. N. Swamy and S. R. Kota (2020), "An Empirical Study on System Level Aspects of Internet of Things (IoT)," in IEEE Access, Vol. 8, pp. 188082-188134.

[2]. L. Xing (2021), "Cascading Failures in Internet of Things: Review and Perspectives on Reliability and Resilience," in IEEE Internet of Things Journal, Vol. 8, No. 1, pp. 44-64.

[3]. Xiuwen Fu, Yongsheng Yang (2021), "Modeling and analyzing cascading failures for Internet of Things," in Information Sciences, Vol. 545, pp. 753-770.

[4]. Fu, P. Pace, G. Aloi, W. Li and G. Fortino (2022), "Cascade Failures Analysis of Internet of Things Under Global/Local Routing Mode," in IEEE Sensors Journal, Vol. 22, No. 2, pp. 1705-1719.

[5]. J. Shehu Yalli, M. Hilmi Hasan and A. Abubakar Badawi (2024), "Internet of Things (IoT): Origins, Embedded Technologies, Smart Applications, and Its Growth in the Last Decade," in IEEE Access, Vol. 12, pp. 91357-91382.

[6]. K. Zia, A. Chiumento and P. J. M. Havinga (2022), "AI-Enabled Reliable QoS in Multi-RAT Wireless IoT Networks: Prospects, Challenges, and Future Directions," in IEEE Open Journal of the Communications Society, Vol. 3, pp. 1906-1929.

[7]. M. Adam, M. Hammoudeh, R. Alrawashdeh and B. Alsulaimy (2024), "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems," in IEEE Access, Vol. 12, pp. 57128-57149.

[8]. Naseer, M. Shmoon, T. Shakeel, S. Ur Rehman, A. Ahmad and V. Gruhn (2024), "A Systematic Literature Review of the IoT in Agriculture—Global Adoption, Innovations, Security, and Privacy Challenges," in IEEE Access, Vol. 12, pp. 60986-61021.

[9]. M. Talebkhah, A. Sali, M. Marjani, M. Gordan, S. J. Hashim and F. Z. Rokhani (2021), "IoT and Big Data Applications in Smart Cities: Recent Advances, Challenges, and Critical Issues," in IEEE Access, Vol. 9, pp. 55465-55484.

[10]. Y. Chi, Y. Dong, Z. J. Wang, F. R. Yu and V. C. M. Leung (2022), "Knowledge-Based Fault Diagnosis in Industrial Internet of Things: A Survey," in IEEE Internet of Things Journal, Vol. 9, No. 15, pp. 12886-12900.

[11]. L. Xing (2020), "Reliability in Internet of Things: Current Status and Future Perspectives," in IEEE Internet of Things Journal, Vol. 7, No. 8, pp. 6704-6721.

[12]. Vishwakarma, A.K., Chaurasia, S., Kumar, K. et al. (2025) "Internet of things technology, research, and challenges: a survey," in Journal of Multimedia Tools and Applications, Vol. 84, pp. 8455–8490.

[13]. Ben Hafaiedh, I., Elaoud, A. & Maddouri, A. (2024) "A formal model-based approach to design failure-aware Internet of Things architectures," in Journal of Reliable Intelligent Environments, Vol. 10, pp. 413–430.

[14]. Moussa Aboubakar, Mounir Kellil, Pierre Roux (2022), "A review of IoT network management: Current status and perspectives", Journal of King Saud University - Computer and Information Sciences, Vol. 34, pp. 4163-4176.