A Framework Design and Solutions Taxonomy for Performance Optimization in Internet of Things Network

Mariam A. Alotaibi[1], Sami S. Alwakeel[2], Aasem N. Alyahya[3]
Department of Computer Engineering-College of Computer Science, King Saud University, Saudi Arabia[1,2,3]
Department of Computer Science and Information Technology, Shaqra University, Saudi Arabia[1]

***Abstract*—The Internet of Things (IoT) is an exciting, rapidly expanding technology that's still in its early stages and faces several complex issues. These challenges primarily arise from the limitations of IoT devices (e.g., restricted energy, memory, and processing power), the diversity of communication protocols, and the heterogeneity of interconnected devices. Collectively, these issues often hinder overall IoT system performance, prompting extensive research into techniques to improve Quality of Service (QoS), particularly in terms of latency, throughput, and energy use. This paper introduces a conceptual framework for multi-dimensional IoT performance optimization. The framework provides a structured approach for evaluating and enhancing performance across all layers of the IoT architecture: device, network, support, and application. It assesses key performance dimensions—reliability, security, scalability, energy efficiency, quality assurance, and enabling technologies—and defines them in terms of overall system performance. To ensure a systematic assessment, these dimensions are supported by concrete performance metrics and precise measurement criteria. Finally, the paper provides a taxonomy of IoT Performance Optimization Components, identifies the essential prerequisites and core attributes that influence the overall efficiency of IoT systems, and thus provides a structured foundation for evaluating and advancing performance across the entire IoT ecosystem.**

***Keywords*—IoT performance; reliability; security; scalability; quality; energy efficiency; technology**

I. Introduction

A. Background and the Rise of the Internet of Things (IoT)

In recent decades, there has been a significant surge in innovative applications centered around mobile actuators, devices, and sensors, enabling complex tasks and pervasive communication [1]. This period of growth reached a major turning point around 2008, when the number of connected devices first surpassed the global population [2]. Today, the interconnection of wireless sensors, smartphones, embedded systems, and various electronic devices via local networks or the Internet has fully ushered in the era of the Internet of Things (IoT).

As the quantity of IoT devices continues to burgeon, the sheer volume of data they generate escalates proportionally. Forecasts anticipate sustained, exponential growth; for example, Cisco projected over 50 billion IoT devices by 2020 and more than 500 billion by 2023 [3] [4]. This promising outlook has naturally spurred considerable financial investment [5].

B. Identifying Critical IoT Challenges and Research Imperatives

Despite this rapid expansion, several persistent challenges hinder the seamless integration of IoT across various industries. These critical issues include reliability, mobility, trust, scalability, security, performance, interoperability, and availability [6] [7] [8].

These challenges highlight significant research imperatives crucial for successfully advancing IoT technologies into diverse sectors like businesses, homes, healthcare, and smart cities, where decisions often carry profound implications for individuals' lives [8]. Consequently, these pressing issues have attracted widespread attention from researchers, prompting intensified and comprehensive efforts to address them. This heightened focus is a direct result of the extensive deployment and utilization of IoT technologies across various spheres of daily life.

C. Defining and Measuring Performance in IoT Systems

The concept of performance and its measurement remains a subject of debate among researchers, with varying perspectives on its precise definition. As suggested by [9], certain scenarios exhibit greater sensitivity to specific parameters when assessing performance metrics. Broadly, performance refers to the system's capability to execute tasks effectively while efficiently conserving system resources.

In the context of IoT, evaluating performance typically involves utilizing established metrics within each architectural layer: At the device layer, metrics may encompass battery lifetime, fault tolerance, failure rates, link reliability, and connectivity.In the network layer, evaluation involves parameters such as delay, throughput, packet loss rate, latency, bandwidth utilization, response time, availability, reliability, cost, failure rate, and fault tolerance.Performance measures at the support layer may include load balancing.Those at the application layer may focus on software resilience, malfunction mitigation, flexibility, and responsiveness.

However, it is important to acknowledge that additional criteria may also warrant consideration due to the unique characteristics of IoT systems.IoT systems are tasked with critical functions such as data collection, data preprocessing, and facilitating machine-to-machine (M2M) communications, among others, as highlighted by [10]. Given their integral role in managing vital infrastructures like healthcare systems and home security, the reliability and security of IoT devices are paramount. Any lapses in reliability or security can have profound implications for decision-making processes, potentially resulting in catastrophic outcomes (Menter et al., 2021).

Enhancing reliability, security, scalability, energy efficiency, and quality assurance represents clear avenues for bolstering the overall performance of IoT systems. The prioritization of performance measurement criteria, however, may vary depending on the system's intended purpose. For instance, in smart home environments, preserving customer privacy may take precedence over other considerations, followed by reliability, energy conservation, and scalability. Conversely, in healthcare systems, reliability and security may assume equal importance. Thus, achieving optimal IoT performance necessitates striking a delicate balance and synergy among these requirements.

D. Scope and Contribution of this Review

This paper presents a conceptual framework for multi-dimensional IoT performance optimization. The proposed framework provides a structured approach for evaluating and enhancing performance across all layers of the IoT architecture, including the device, network, support, and application layers. It evaluates key performance dimensions—reliability, security, scalability, energy efficiency, quality assurance, and enabling technologies—and defines them in terms of the overall system performance. These dimensions are further supported by concrete performance metrics identification and measurement criteria, offering a comprehensive basis for systematic performance assessment and improvement.

The remainder of this paper is organized as follows. Section II reviews existing research contributions and classifies IoT performance-enhancement solutions across different architectural layers. Section III presents the proposed conceptual framework and explains its multi-dimensional structure. Section IV introduces the taxonomy of performance-impact components and analyzes their relevance to IoT optimization. Section V summarizes prominent suggested solutions derived from the surveyed literature. Section VI provides a detailed discussion of key insights, highlights research gaps, and outlines future research directions. Finally, Section VII concludes the paper.

II. Key Research Studies Solutions for IoT System Performance Enhancement

Numerous studies have made significant efforts to enhance the performance of the IoT system. Solutions are suggested for optimizing various metrics of a particular IOT system dimension, such as reliability, security, scalability, energy efficiency, or quality of service (QoS). This section reviews key studies that have proposed solutions to enhance the performance of various dimensions of IoT systems.

A. Reliability-Oriented Solutions

Reliability remains a core requirement in IoT systems, as even minor sensing or communication errors can disrupt critical applications, particularly in healthcare and safety monitoring. Existing research has approached IoT reliability from multiple architectural perspectives, with solutions spanning the application, support, network, and device layers.

At the application layer, several studies leverage microservice-based designs to enhance availability and fault isolation. Reactive microservices were employed in study [11] to improve runtime stability in smart agriculture applications, while [12] demonstrated that re-engineering monolithic IoT middleware into loosely coupled microservices increases reliability, maintainability, and scalability. Complementing these architectural strategies, the Circuit Breaker pattern explored in study [13] prevents cascading failures across dependent services, thereby strengthening fault tolerance in IoT communication workflows.

At the support layer, reliability has been enhanced through middleware mechanisms that improve fault tolerance across cloud–fog–edge environments. For instance, [14] introduced middleware services that support resilient operation in latency-sensitive smart city applications, ensuring continuous service delivery even under partial platform failures.

At the network layer, research largely centers on fault-tolerant routing. The CHISS model in study [15] evaluates routing reliability using metrics such as path redundancy, subsystem availability, and data/service readiness, while healthcare-focused architectures such as [16] introduce backup routes and adaptive strategies to preserve connectivity during node or link failures. Optimization-based techniques, such as the PMSO multipath routing algorithm in study [17], further improve robustness by constructing and maintaining multiple disjoint paths that sustain connectivity under successive failures.

At the device layer, reliability enhancements focus on accurate data acquisition and resilient on-device processing. Device evaluation frameworks in [18] and [19] estimate hardware and operational reliability using recognition, classification, probabilistic modeling, and validation stages. Additional works strengthen dependability in healthcare monitoring [20], enable fault-tolerant microservice execution on IoT–Cloud environments [21], and integrate online learning for proactive fault mitigation [22]. Edge-focused frameworks such as Achlys [23] support reliable decentralized computation on resource-constrained devices, while redundancy techniques like Cold Standby Sparing (CSSR) [24] significantly improve device-level fault tolerance.

Overall, existing reliability solutions target different IoT layers but show recurring themes: architectural decomposition at the application layer, resilient middleware at the support layer, fault-tolerant routing at the network layer, and hardware/software robustness at the device layer. These collective findings highlight the multi-layered nature of reliability challenges in IoT environments.

B. Security-Oriented Solutions

Security is essential to preserving integrity, confidentiality, authenticity, and privacy across IoT deployments. Existing research has addressed IoT security at multiple architectural layers, proposing mechanisms that strengthen software robustness, enforce access control, secure communication protocols, and protect resource-constrained devices.

At the application layer, several studies improve software-level security through structured design patterns and policy-driven enforcement. Works such as [25]–[27] refine and apply security patterns—including access control, reference monitoring, and remote authentication—to mitigate risks in IoT software systems and event-driven applications. Policy-based solutions such as IOTGUARD [28] and SecKit-MQTT [29] embed runtime monitoring, behavioral modeling, and privacy rule enforcement directly into IoT applications, preventing unsafe interactions and safeguarding personal data even in constrained user-facing environments. User-centric regulatory compliance is addressed in study [30], which assesses privacy policy completeness under GDPR requirements. Access control enhancements such as iLACKA-IoT [31] provide formally verified authentication and authorization with improved computational efficiency. Other protocol-level protection mechanisms include secure extensions of MQTT/MQTT-SN using Elliptic Curve–based KP/CP-ABE encryption in study [32], blockchain-integrated microservice architectures for secure surveillance [33], and lightweight certificateless /identity-based signcryption for healthcare WBANs [34].

At the support layer, security research focuses on dependable cloud–fog–edge infrastructures. The Markov-based modeling framework in [35] quantifies system compromise, availability, and recovery behavior for medical IoT systems. Secure data management solutions include cloud–fog–edge cache decision systems [36] that safeguard large-scale smart building data over 6G networks, and privacy-preserving deduplication protocols [37] that protect stored data equality and confidentiality during distributed fog–cloud storage operations.

At the network layer, numerous studies reinforce secure routing and communication. Crypto-IoT [38] and KMG [39] introduce lightweight key generation, distribution, and authentication to protect unicast/multicast communication while maintaining low energy consumption. RPL-based enhancements include SPLIT [40], which integrates remote attestation without adding control overhead, and SARP [41], which provides scalable integrity verification for heterogeneous IoT devices. Additional secure routing techniques include ESR [42], which combines energy-efficient clustering with threshold secret sharing, and SRR [43], which protects source-location privacy using randomized phantom routing. Internetworking security is addressed in [44] via combined Diffie–Hellman, AES, and MD5 mechanisms, and in [45] through lightweight HMAC-based authentication schemes that achieve robust integrity and confidentiality with minimal latency.

At the device layer, security solutions target constrained sensors and local data protection. Information-theoretic coding schemes [46] preserve message confidentiality and anonymity without synchronization overhead, while SecureData [47] employs FPGA-accelerated lightweight ciphers and data-splitting techniques to protect sensitive healthcare information. Other lightweight device-level protection mechanisms, including HMAC-based authentication [45] and secure data aggregation surveys [48], strengthen confidentiality, integrity, and authentication during sensing and in-network processing.

Overall, IoT security solutions span all architectural layers, with recurring themes such as pattern-driven software hardening at the application layer, privacy- and integrity-focused middleware at the support layer, attestation and key management mechanisms at the network layer, and lightweight cryptographic protection for resource-constrained devices. These contributions highlight the multi-layered and interdependent nature of IoT security challenges.

C. Scalability-Oriented Solutions

Scalability is a critical requirement in IoT systems, as large-scale deployments must maintain responsiveness, manage resource constraints, and support heterogeneous device interactions. Research efforts addressing scalability span multiple IoT layers, proposing architectural, orchestration, and routing solutions.

At the application layer, Razzaq [49] provides a comprehensive review of microservice-based architectures (MSA), identifying key design patterns and architectural trends that enhance scalability and software quality in IoT applications. Context-aware and personalized service delivery is explored in [50], where adaptive sensing, fog-based user-centric networking, and intelligent applications together support scalable, interoperable, and context-driven IoT services. Zyrianoff et al. [51] further demonstrate that large-scale smart city environments can sustain real-time reasoning when architectural choices emphasize modularity, efficient context handling, and optimized system design.

At the support layer, scalability improvements primarily target cloud–fog–edge integration and resource orchestration. Lightweight sidecar components in [52] enable seamless device-to-cloud interaction without modifying device behavior, providing modular extensibility for large-scale deployments. Ontology-driven integration frameworks such as IoT-LSS [53] combine SOA and semantic sensor models to support scalable interoperability and dynamic service composition. Transparent computing architectures in [54] manage operating systems, services, and data centrally while enabling on-demand execution across heterogeneous IoT devices, improving scalability and energy efficiency. Surveys and analyses in [55] and [56] highlight the pivotal role of auto-scaling, load prediction, VM migration, and multi-layer orchestration in cloud–edge environments, demonstrating that scalable performance depends heavily on efficient, network-aware resource allocation.

At the network layer, scalability challenges are tackled through enhanced routing protocols. IoTorii [57] introduces a hierarchical routing approach that reduces control overhead and routing table complexity compared to RPL, achieving faster convergence and lower communication costs in large-scale deployments. Complementary to this, secure and scalable RPL extensions such as SPLIT [40] and SARP [41] integrate lightweight attestation and decentralized trust mechanisms, improving routing efficiency while maintaining security and low resource consumption.

Overall, scalability solutions in IoT emphasize modular architectures, semantic interoperability, cloud–edge orchestration, and optimized routing mechanisms. These contributions highlight that scalability must be addressed holistically across application, support, and network layers to sustain the performance of large and heterogeneous IoT systems.

D. Quality Assurance-Oriented Solutions

Quality assurance in IoT systems ensures that data and services remain accurate, timely, and dependable despite dynamic operating conditions. Research addressing IoT quality spans the application, support, and network layers, targeting metrics such as latency, throughput, availability, and service reliability.

At the application layer, Li et al. [58] introduce measurable data-quality metrics—currency, availability, and validity—to assess both data and source reliability in pervasive IoT environments. These metrics enable systems to manage fluctuating real-time data and improve application-level decision-making. QoS-aware microservice monitoring for Industrial IoT (IIoT) is explored in [59], where microservices are evaluated based on behavioral performance, supporting consistent and dependable execution of IIoT workloads.

At the network and support layers, QoS has been analyzed broadly through systematic mapping and metric categorization. White et al. [60] review QoS approaches across IoT layers, identifying common performance factors (e.g., latency, throughput, availability) and highlighting underexplored QoS dimensions and research gaps. Singh et al. [61] similarly classify QoS metrics spanning computing, communication, and physical components, providing a structured basis for modeling service requirements and optimizing IoT performance. Fog-enabled quality improvement is demonstrated in SmartHerd [62], where localized processing reduces cloud dependency, lowers latency, and decreases bandwidth consumption by 84%, contributing to higher service responsiveness and energy efficiency.

At the network layer, congestion control and traffic stabilization play a key role in maintaining quality. Quwaider et al. [63] propose a tuned PID-based congestion control mechanism enhanced by immune and hill-climbing algorithms. The scheme stabilizes buffer occupancy, minimizes packet drops, and ensures steady throughput and low delay under dynamic traffic conditions.

Overall, quality assurance solutions in IoT focus on measurable data-quality metrics, QoS-aware service design, fog-enabled responsiveness, and congestion-aware communication, illustrating the layered and multi-dimensional nature of quality management in IoT systems.

E. Energy Efficiency-Oriented Solutions

Energy efficiency is essential in IoT deployments, where devices often operate under strict energy constraints and in unattended environments. Existing research addresses energy conservation across all IoT architectural layers, focusing on optimizing operations, communication, processing, and resource orchestration.

At the application layer, energy-aware service policies contribute directly to reducing consumption. Yao et al. [64] introduce a Home Energy Management System (HEMS) using mixed-integer linear programming to jointly optimize appliance scheduling, renewable energy usage, and storage dispatch, reducing energy costs while maintaining user comfort.

At the support layer, numerous studies emphasize cloud–fog–edge coordination and resource orchestration for energy-efficient IoT services. Energy-efficient cooling automation based on containerized microservices is demonstrated in [65], showing how lightweight orchestration enables reliable and power-saving IoT–cloud integration. Sensor-cloud collaboration models in [66] offload complex processing to the cloud while dynamically scheduling sensor activity, conserving energy while meeting latency constraints. Architectures integrating cloud computing with Passive Optical Networks (PON) [67] optimize VM placement and traffic routing to minimize transmission and computation power. Fog-based placement optimization in healthcare monitoring [68] achieves up to 68% energy savings by strategically locating fog servers. Resource orchestrators in study [69] and [70] improve the efficiency of service embedding and cloud resource scheduling, reducing network and processing power through adaptive allocation and predictive sensor sleep cycles.

At the network layer, energy-efficient communication is achieved through optimization-based routing and flow control. Al et al. [71] present four MILP-based strategies—standby routing, reliability balancing, interference-aware sub-channels, and data compression—to reduce power consumption while maintaining reliability. For industrial IoT, Lyu et al. [72] propose a transmission–estimation co-design framework that adapts communication decisions based on dynamic system conditions, enhancing estimation accuracy with lower energy usage. Secure and energy-efficient uplink transmission is addressed in study [73], where cooperative relay selection and joint power scheduling improve secure energy efficiency under eavesdropping threats. Network-layer energy management also includes call admission control (CAC) for ultra-dense IoT over 5G, as proposed in study [74], reducing per-connection energy consumption through intelligent access decisions.

At the device layer, lightweight communication and in-network processing reduce energy demand on constrained sensors. Purkovic et al. [75] design an ultra–low-power long-range communication protocol that minimizes packet overhead and transmission energy for energy-harvesting IoT modules. Complementing this, [76] surveys energy-aware data aggregation schemes that eliminate redundancy and reduce communication load across diverse WSN environments—ground, underground, and underwater—extending network lifetime through efficient data collection.

Overall, energy efficiency solutions span application-level policy optimization, fog–cloud orchestration, power-aware routing and flow control, and device-level communication minimization. These cross-layer techniques collectively highlight the importance of coordinated architectural design for prolonging IoT system lifetime.

F. Summary of Literature-Based IOT Performance Enhancement Solutions

To conclude this review section, Table I presents a consolidated view of the surveyed literature references for IoT performance enhancement solutions. It provides an easy reference classification that relates a proposed reference solution to a given performance IoT dimension. Each referenced study is categorized according to its specific IoT system performance dimension, namely: reliability, security, scalability, quality, or energy efficiency, alongside the corresponding IoT architectural layer (Device, Network, Support, or Application) and the targeted component or service. This structured representation in Table I facilitates a clear understanding of how recent research efforts align with key architectural and performance considerations across the IoT stack while identifying underexplored areas that warrant further investigation that this thesis research may address.

III. Conceptual Framework Design and Literature Taxonomy for IoT Performance Optimization

The proposed framework provides a structured approach for evaluating and enhancing performance across all layers of the IoT architecture, including the device, network, support, and application layers. It evaluates key performance dimensions, reliability, security, scalability, energy efficiency, quality assurance, and enabling technologies, and defines them in terms of the overall system performance. These dimensions are further supported by concrete performance metrics identification and measurement criteria, offering a comprehensive basis for systematic performance assessment and improvement.

A. IoT Performance Framework Design

The IoT performance optimization framework design follows a systematic approach, as illustrated in Fig. 1. The process involves five primary steps that ensure comprehensive coverage of the IoT architecture. These steps are:

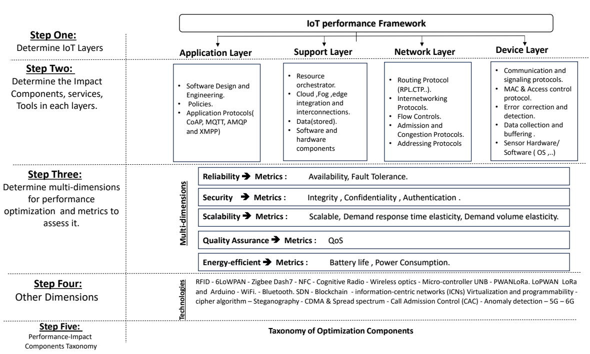

Fig. 1. IoT performance framework design steps.

- Step One: Determine IoT layers.
  In this step, the core layers of the IoT architecture are identified, including the application layer, support layer, network layer, and device layer. These layers form the basis for the subsequent optimization strategies.
- Step Two: Determine the impact components, services, and tools in each layer.
  This step identifies the components, services, and tools of each layer that impact overall performance. For example, the application layer considers software design and engineering tools, while the network layer incorporates routing protocols like RPL and CTP.
- Step Three: Determine the multi-dimensional factors for performance optimization.
  Multi-dimensional factors such as reliability, security, scalability, quality assurance, and energy efficiency are considered in this step. The relevant metrics for each dimension are defined, including factors like availability, fault tolerance, and battery life.
- Step Four: Other dimensions.
  Additional factors that influence performance, such as emerging technologies (e.g., 5G, LoRaWAN, WiFi), are evaluated in this step.
- Step Five: Taxonomy of optimization components.
  In this step, various components impacting IoT performance optimization are analyzed and classified. The analysis concludes a structured, taxonomy for performance-impact components across a multi-layer and multi-service IoT architecture of the performance framework.

Fig. 1 illustrates the overall structure of the proposed multi-dimensional IoT performance framework. The figure highlights the interaction between IoT architectural layers (Device, Network, Support, and Application) and the core performance dimensions (Reliability, Security, Scalability, Quality, and Energy Efficiency). Each layer contributes to these performance dimensions through specific components, services, or mechanisms. Importantly, the framework enables each dimension to be evaluated and measured at the corresponding layer using the performance metrics defined in Step Three. These metrics help determine whether a given performance requirement—such as availability, fault tolerance, latency, or energy consumption—is being achieved at that layer.

The directional flow emphasizes cross-layer dependencies, demonstrating that improvements in one layer may influence performance at other layers. This visual representation provides the conceptual foundation for the taxonomy introduced in the subsequent section, where performance-impact components are categorized and linked to measurable metrics across layers.

B. IoT Network Performance-Relevant Layers

The architecture of IoT is commonly structured into four fundamental layers: the device, network, support, and application layers. While each layer plays a distinct role in enabling end-to-end communication and intelligent decision-making, this framework focuses on how these layers form the basis for performance evaluation.

- Device Layer: Serves as the foundational interface with the physical world. Performance at this level is driven by hardware and software elements such as sensor nodes, embedded operating systems, and data collection modules.
- Network Layer: Determines performance through routing and communication infrastructure, relying on routing protocols (e.g., RPL, CTP), internetworking protocols, and addressing schemes to ensure reliable packet delivery.
- Support Layer: Provides computing, storage, and orchestration capabilities, including cloud–fog–edge integration and resource orchestrators that manage distributed resources to improve reliability and responsiveness.

TABLE I. LITERATURE-BASED CLASSIFICATION OF SOLUTIONS TARGETING IOT PERFORMANCE DIMENSIONS

Layer	Impact Component, Tools, Service	Reliability	Security	Scalability	Quality	Energy Efficiency
Application Layer	Software Design and Engineering	[11]	[25] [26] [27]	[49] [50] [51]		
	Policies		[28] [29] [30] [31]	[51]		
	Application Protocols	[12] [13]	[33] [32] [31] [34]		[58] [59]	[64]
Support Layer	Resource Orchestrator			[53] [54] [55] [56]	[55] [60] [61]	[55] [65] [69] [70]
	Cloud/Fog/Edge Integration	[14]	[36]	[50] [52] [55] [56]	[62] [55]	[55] [66] [67] [68]
	Data (stored)		[37]			
	Software/Hardware Components		[35]			
Network Layer	Routing Protocol	[15] [16] [17] [71]	[38] [39] [40] [41] [42] [43]	[40] [41] [42] [57]	[61]	[39] [40] [41] [42] [43] [71]
	Internetworking Protocols		[45] [44]			
	Flow Control					[72] [73]
	Admission and Congestion Control				[63]	[74]
	Addressing Protocols					
Device Layer	Communication and Signaling		[45]			[45] [75]
	MAC and Access Control		[46]			
	Error Correction and Detection					
	Data Collection and Buffering		[48]			[76]
	Sensor Hardware and Software	[18] [19] [20] [21] [22] [23] [24]	[47]	[50]		

- Application Layer: Functions as the user interface, depending on efficient software design, lightweight protocols (e.g., CoAP, MQTT), and policies that govern usability, adaptability, and security.

These architectural layers form the foundation for evaluating and optimizing IoT performance across multiple dimensions, each providing distinct enhancement opportunities.

C. IoT Network Performance-Relevant Services, Components and Tools

Beyond the layered architecture, IoT performance is also shaped by the specific services, components, and tools operating within each layer. These elements provide the practical mechanisms through which performance optimization is achieved. The device layer Comprises Key components, including communication and signaling protocols, MAC and access control mechanisms, and error detection and correction techniques, all working together to ensure reliable and efficient data acquisition. Additionally, data buffering mechanisms support seamless transmission preparation, significantly minimizing energy consumption and preserving data accuracy. At the network layer, Key components include routing protocols (e.g., RPL, CTP), internetworking protocols, and addressing schemes, all essential for ensuring reliable packet delivery and supporting system performance. Further performance optimization is achieved by implementing flow control, admission control, and congestion control mechanisms, which collectively regulate network load and maintain consistent data throughput under varying traffic conditions. The support layer includes a key element, the resource orchestrator, which dynamically schedules and manages computational and storage resources. Furthermore, the software and hardware infrastructure and dedicated data storage components ensure IoT services' reliability, availability, and responsiveness across distributed environments. Finally, the application layer. Its performance depends on effective software engineering practices, the adoption of lightweight and reliable application-layer protocols (such as CoAP, MQTT, AMQP, and XMPP), and well-defined policies that govern service behavior and access control. Design decisions made at this layer directly influence the responsiveness, usability, and adaptability of IoT applications across various domains. By systematically identifying these performance-relevant services, components, and tools in each layer, the framework links the conceptual architecture of IoT with the operational elements that directly impact system efficiency and optimization.

D. Multi-Dimensional Performance Requirements and Metrics

This section presents the multi-dimensional requirements of IoT performance optimization and the corresponding performance metrics and measures. It first identifies the key performance dimensions, such as reliability, scalability, energy efficiency, security, and quality assurance, which are critical to achieving optimized IoT network behavior. Subsequently, it defines specific metrics and measures that quantify these dimensions and enable objective evaluation and comparison of IoT systems.

1) Reliability Dimension Performance Requirement and Metrics: Reliability is a fundamental requirement for IoT performance, as unreliable components or services, such as processing, transmission, and sensing can lead to significant system failures, delays, and loss of data or communication. These issues have profound implications for IoT systems' overall performance and stability. Given the emerging nature of IoT technologies, it is essential to define the concept of reliability clearly within this context. Unlike fields such as engineering and software engineering, where reliability is well-established, there remains no universally agreed-upon definition specific to IoT [77].

According to study [78], reliability can be defined as the probability that a component or system will meet specific performance standards by yielding correct output over a desired period under given environmental conditions. In essence, reliability encompasses the study of system failures, their causes, mitigation strategies, and methods for failure prevention.

Since IoT systems consist of hardware and software components that often interact autonomously, human factors must also be considered when evaluating reliability. Thus, IoT reliability is influenced by hardware failure rates and software robustness, standardization challenges, and human interaction [78].

In study [79], the author identifies four essential requirements for achieving reliability in IoT devices:

- Performing a required function.
- Performing without failure.
- Operating under stated conditions.
- Operating for a specified period of time.

Building on this, Mavrogiorgou et al. [18] highlight that when specifying and designing for reliability, it is essential to define the expected conditions of use, what constitutes proper operation, and what qualifies as a failure. They emphasize the importance of clearly describing the system's functionality, the operational environment, and the timescale for assessing how well the system meets its intended specifications. Similarly, the author in study [80] emphasizes that reliability should be understood as the consistent performance of a device or system over a specified period.

Overall, reliability in IoT requires a multifaceted approach that integrates hardware resilience, software robustness, human factors, and standardization efforts to ensure sustainable system performance. To assess and improve IoT reliability, it is necessary to adopt specific metrics and measures that quantify this dimension.

Reliability is typically denoted by R(t) and can be measured using several metrics [77] [81] [82] [83]. Key metrics include:

- Mean Time Between Failures (MTBF)
- Mean Time to Failure (MTTF)
- Maintenance-Free Operating Period (MFOP)
- Maintainability
- Availability
- Failure Rate

One of the key metrics for reliability is Availability, which represents the probability that a system will operate correctly during a given period. It is calculated using the following Eq. (1):

$$A = \frac{MTTF}{MTTF + MTTR} \tag{1}$$

Where: MTTF is the Mean Time to Failure and MTTR is the Mean Time to Repair.

From the Eq. (1), it can be seen that a higher MTTF leads to higher reliability and availability. However, high availability does not always equate to high reliability. If the system is repaired quickly, with a low MTTR, it may maintain availability, but this does not necessarily reflect the system's overall reliability. Reliability can also be measured in different ways depending on the system's recovery mechanism:

- For systems with no recovery mechanism, the system cannot repair itself once a failure occurs, and operation stops until manually restored. In such cases, MTTF is used to measure reliability, as the system's availability and reliability are the same based solely on the time it operates without failure before a breakdown [81], and can be calculated as Eq. (2) illustrated:

  $$\lambda = \frac{1}{MTTF} \tag{2}$$

  where λ represents the failure rate, defined as the expected number of failures per unit time.
- For a system that can be maintained, reliability is measured by the MTBF, calculated as Eq. (3):

$$\lambda = \frac{1}{MTBF} \tag{3}$$

Finally, to quantitatively system reliability over time, the reliability function R(t) is introduced in Eq. (4):

$$R(t) = e^{-\lambda t} \tag{4}$$

This function provides a formal means to describe the probability that a system or component will continue to perform without failure up to a given time t, following an exponential decay pattern. This formulation is commonly used to represent the reliability of individual components under the assumption of random, time-independent failures. However, IoT systems typically have multiple interdependent elements, including hardware, software, and human interaction components. Therefore, Eq. (5) extends this concept by aggregating the reliabilities of these distinct elements to estimate the overall system reliability, $R_{\text{S}}(t)$.

$$R_s(t) = R_{HW}(t) + R_{SF}(t) + R_H(t) \tag{5}$$

Each component reliability, $R_{\text{HW}}(t)$ for hardware, $R_{\text{SF}}(t)$ for software, and $R_{\text{H}}(t)$ for human factors, can individually be modeled using the exponential form described in Eq. (4). Thus, Eq. (5) highlights that the system's reliability depends on the combined contribution of its key parts, each following its failure behavior over time [81].

2) Security Dimension Performance Requirement and Metrics: Security has become a significant concern that significantly affects the performance of IoT networks, particularly as the number and sophistication of attacks continue to grow. According to [84], IoT networks are inherently more vulnerable than traditional networks due to the unique attributes of IoT devices and the communication protocols they employ. For instance, IoT devices are often equipped with low-power microcontrollers and limited battery capacities, making them susceptible to resource exhaustion attacks. Moreover, they communicate over protocols such as GSM, Bluetooth, Wi-Fi, and ZigBee, which are more prone to attacks.

Security measures in IoT systems aim to reduce the probability of successful attacks and minimize security risks. A secure system ensures that unauthorized access is prevented, resources are protected, and operational integrity is maintained. By preventing malicious actors from accessing or exploiting system resources, the IoT system can continue to perform its tasks efficiently and reliably. Attacks such as Denial of Service (DoS) or resource exploitation can severely degrade system performance by causing system failures or slowing down operations through the exhaustion of memory, processing power, or storage. Consequently, maintaining security is critical to ensuring IoT systems function perfectly while balancing the trade-off between security and system performance [85].

To foster IoT security, Aman et al. [86] outlined several essential mechanisms that can be applied:

- All IoT devices operating within a network should run authorized and verified software.
- Devices must be authenticated to verify their legitimacy before transmitting or receiving data.
- Packet filtering via firewalls at the device level is recommended to compensate for limited computational and memory capacities.
- Regular updates and security patches must be applied to ensure protection against newly discovered vulnerabilities.

For optimal performance of IoT systems, applications and services must be secured, user privacy must be safeguarded, and threats such as spoofing and data manipulation must be prevented. Furthermore, IoT systems should operate independently without overreliance on external systems to maintain resilience [87].

Several fundamental security measures must be enforced across IoT ecosystems, including integrity, confidentiality, and authentication [82], [86], [87].

Confidentiality is a fundamental security measure that ensures data is accessible only to authorized users [87]. It protects against unauthorized interception or access to sensitive information transmitted between IoT devices [88]. Encryption and access validation mechanisms are essential to enforce confidentiality [89]. For example, sensor nodes must prevent neighboring nodes from accessing collected data, and RFID tags must safeguard sensitive information from unauthorized readers [87].

Integrity ensures that data remains consistent, accurate, and unaltered during transmission or storage, protecting against tampering by malicious users or software [86].

Authenticity ensures the data source is legitimate and trustworthy [87], [90]. Authentication processes must be implemented at every layer of the IoT architecture to prevent unauthorized nodes from injecting false information. For instance, sensor nodes must authenticate themselves at the device layer to avoid DoS attacks caused by rogue devices [91]. Robust authentication mechanisms are critical for maintaining system security across all layers.

IoT systems must carefully balance privacy, confidentiality, integrity, authenticity, and performance trade-offs without introducing unnecessary dependencies or vulnerabilities [86]. Strengthening these security measures is vital to safeguarding IoT ecosystems and ensuring their resilient, efficient, and reliable operation.

3) Scalability Dimension Performance Requirement and Metrics: Due to the rapid expansion of IoT technologies and the enormous volume of data generated by these devices, it has become imperative to develop strategies for accommodating this massive scale without necessitating a complete reengineering of existing systems. **Scalability** is a fundamental characteristic of any system that must manage an increasing workload efficiently; a lack of scalability can lead to degraded performance, increased latency, inefficient resource consumption, and poor utilization of available infrastructure. Achieving scalability presents significant challenges, particularly as a single IoT application often connects to many heterogeneous devices. Thus, extendable and flexible operations are essential to manage the distribution and functionality of these devices effectively [86].

According to study [92], scalability is defined as the ability of a system or device to adapt to environmental changes and meet future demands without compromising performance. Furthermore, scalability is recognized as an integral component of the broader performance requirements for IoT services, which places increased pressure on researchers and developers to devise solutions capable of handling the vast and growing volumes of data [93]. Scalability can manifest at both the hardware and software levels: horizontal scalability involves expanding the network by adding additional hardware devices or software entities, thereby distributing the workload across a broader system, whereas vertical scalability refers to enhancing the capabilities of existing devices or programs by integrating additional resources, such as computational power or storage capacity [94].

For optimal performance, it is essential to implement scalable solutions capable of managing millions of users and service requests simultaneously. Several researchers have explored methods for evaluating and measuring scalability in this context. One commonly used method involves assessing the system's latency and throughput under varying loads. Ideally, in a scalable system, latency remains stable even as the number of servers increases. In contrast, throughput proportionally increases with the addition of servers, meaning the system is able to process more requests concurrently [95]. Another scalability metric discussed in [96] evaluates the system's ability to dynamically increase the number of software instances to meet the rising demand for services. Importantly, scalable systems are expected to maintain the same average response time and consistent QoS regardless of the volume of service requests, ensuring reliability even under heavy loads. Thus, scalability is essential for supporting the expanding IoT ecosystem and a critical determinant of a system's long-term success and performance stability.

4) Service Quality Dimension Performance Requirement and Metrics: The quality of IoT systems plays a pivotal role in ensuring overall system performance and achieving the required QoS levels. However, maintaining high quality across IoT ecosystems presents a significant challenge due to the heterogeneity of devices, networks, and platforms. To address these complexities, it is essential to establish a comprehensive framework capable of evaluating each component individually and verifying whether it meets its expected performance and output standards.

QoS in IoT can be broadly defined as the network's ability to deliver an appropriate level of service to meet the specific needs of applications and users [97]. However, QoS requirements in IoT environments are highly variable and largely depend on the intended use case and system architecture. As outlined in [60], QoS expectations can typically be classified into three categories:

- No QoS: Best-effort service with no formal guarantees on performance or delivery.
- Differentiated Services (Soft QoS): Services that prioritize traffic based on application needs but do not guarantee strict performance standards.
- Guaranteed Services (Hard QoS): Services that provide strict guarantees for performance metrics such as delay, bandwidth, and reliability.

Quality and performance are inherently intertwined in IoT systems. While performance refers to the measurable behavior of the system (e.g., response time, throughput), quality encompasses broader aspects such as reliability, user satisfaction, and adherence to service-level agreements. Therefore, achieving high-quality standards is a prerequisite for attaining optimal system performance. In this research, quality was considered a foundational dimension that directly impacts the ability to optimize the IoT system's overall performance and user experience.

QoS requirements in IoT environments vary significantly depending on the specific needs of the system and the nature of the applications involved. To ensure that appropriate service levels are delivered, it is crucial to implement targeted QoS techniques at each layer of the IoT architecture. Each layer has distinct QoS metrics and parameters that contribute to determining the overall service quality.

According to study [97] [60] [98], the quality parameters in IoT can be classified based on architecture layers:

1) QoS at the Application Layer, this layer focuses on application-specific requirements related to the behavior and context of the devices and users:
   - Location and Mobility
   - Sampling Parameters
   - Time Synchronization
2) QoS at the Support Layer, ensures efficient management of computational and storage resources across distributed infrastructures (cloud, fog, edge):
   - Load Balancing
   - Response Time
   - Resource Orchestration
3) QoS at the Network Layer, addresses the performance of data transmission and communication reliability:
   - Jitter
   - Bandwidth
   - Delay
   - Throughput
   - Packet Delivery Time
   - Packet Loss Rate
4) QoS at the Sensing Layer, the sensing layer evaluates the quality and efficiency of data collection and initial processing:
   - Accuracy of Service and Information
   - Cost of Network Deployment and Service Delivery
   - Service Attributes (Priority, Availability, Response Time, Delay, and Load)

Ensuring high-quality service delivery in IoT systems requires a comprehensive understanding of the QoS requirements at each architectural layer. By systematically addressing quality parameters across the application, support, network, and sensing layers, it becomes possible to optimize performance, enhance user satisfaction, and maintain the resilience of IoT ecosystems. This layered approach is foundational to achieving holistic performance optimization in modern IoT environments.

5) Energy Efficiency Dimension Performance Requirement and Metrics: Energy constraints in the IoT ecosystem, particularly regarding limited battery capacities and energy harvesting capabilities, make energy efficiency a critical requirement for maintaining system performance. Inefficient energy management directly impacts core system attributes such as reliability, security, and scalability. Therefore, optimizing energy efficiency is a major research priority in the development of IoT technologies.

Energy efficiency in IoT systems is commonly defined as the number of bits successfully transmitted per joule of consumed energy [99]. It can be mathematically expressed by Eq. (6):

$$\text{Energy Efficiency (EE)} = \frac{\text{Number of Transmitted Bits}}{\text{Energy Consumption (EC) in Joules}} \tag{6}$$

where Energy Consumption (EC) represents the total amount of energy expended by the device during its operation, typically measured in joules. A higher energy efficiency value indicates more effective use of energy resources.

High energy efficiency is crucial for energy-constrained domains such as smart industrial systems, implantable medical devices, and remote environmental monitoring, where continuous maintenance or battery replacement is impractical. For less critical applications, such as consumer sports wearables, moderate energy efficiency levels may be sufficient. Supplying sufficient energy to operate IoT systems autonomously, without degrading other performance requirements, remains a significant implementation challenge. Given the pivotal role of energy in battery-operated IoT devices, extensive research efforts have focused on developing energy-saving mechanisms at both the hardware and system levels.

Energy management is a primary consideration in IoT device design. Strict control over device power consumption is necessary to achieve energy efficiency and preserve the expected battery lifetime. Three key metrics are typically employed to evaluate energy efficiency:

- Energy Consumption (EC): The total energy consumed by the device over its operating period, measured in joules.
- Power Consumption (PC): The rate at which the device uses energy during operation, typically measured in watts.
- Battery Lifetime: The operational duration of the device before requiring battery replacement or recharging, typically measured in hours, days, or years, depending on the application.

Battery lifetime requirements in IoT systems vary widely depending on the application. For instance, consumer wearables may operate for a few days, whereas sensor nodes deployed in remote or hazardous environments are expected to function autonomously for several years. Although advancements in low-power electronics have contributed to reducing individual component energy usage, a holistic understanding of system-wide energy consumption and power profiles remains essential for optimizing overall energy efficiency and extending device operational lifetimes.

E. Technologies Dimension Performance Requirement and Metrics

IoT is an integration of multiple **technologies** working together. Due to the diverse characteristics of IoT systems and the distinct purposes and functions of each architectural layer, various enabling technologies have been proposed in the literature to meet the specific requirements of each layer. IoT deployment in real-world environments is made possible only through the collaboration of these enabling technologies, which collectively enhance overall system performance. Accordingly, this section is dedicated to discussing the key enabling technologies that support and optimize the functionality of IoT systems.

According to study [100], the techniques utilized in IoT systems are categorized into three phases based on their functional roles:

1) Collection Phase: Involves real-time sensing, data gathering, and constructing a comprehensive view of the physical environment using technologies such as RFID, sensors, and NFC.
2) Transmission Phase: Focuses on delivering the collected data to external applications and servers through communication technologies such as wireless networks, satellite links, and Ethernet.
3) Processing, Management, and Utilization Phase: Responsible for analyzing and processing the incoming data streams, forwarding information to applications and services, and generating feedback to control actuators or services. This phase also encompasses critical tasks such as device discovery and management, data filtering, aggregation, analysis, and intelligent decision-making.

Similarly, [101] classified IoT enabling technologies into three functional categories:

1) Technologies responsible for acquiring information.
2) Technologies responsible for processing and managing relevant information.
3) Technologies aimed at enhancing privacy and security.

The first two categories represent the fundamental building blocks necessary for imparting intelligence to "things," distinguishing the IoT from the traditional Internet. In contrast, the third category, privacy and security technologies, is not a functional layer but a critical prerequisite for IoT adoption. Without robust privacy and security mechanisms, IoT systems' widespread deployment and acceptance would be severely constrained [102].

IoT integrates a heterogeneous combination of hardware, software, and communication system technologies. These diverse technologies must be effectively adapted and coordinated to ensure IoT systems' reliability, security, scalability, and energy efficiency. Such adaptation directly enhances the overall performance and resilience of IoT deployments. In this thesis, the enabling technologies are broadly classified into the following categories:

- Hardware and Wireless Technologies
- Software and Algorithmic Solutions
- Machine Intelligence Techniques
- Telecommunication Systems

Table II summarizes the key enabling technologies relevant to the IoT ecosystem, classified based on their technological type, hardware and wireless technologies, software and algorithms, machine intelligence, and telecommunication systems. The table also maps these technologies to their respective contributions across five critical performance dimensions: reliability,

TABLE II. MAPPING OF ENABLING TECHNOLOGIES TO MULTI-DIMENSIONAL IOT PERFORMANCE REQUIREMENTS

	Type	Multi-dimensional requirements for performance optimization				
		Reliability	Scalability	Security	Quality	Energy
Enabling Technologies	Hardware and Wireless	RFID, 6LoWPAN	ZigBee, Dash7, 6LoWPAN, RFID	RFID, NFC, 6LoWPAN	Cognitive Radio, Wireless Optics, CDMA / Spread Spectrum	Microcontrollers (UNB), LoRa, LPWAN, Arduino with ZigBee, WiFi, Bluetooth
	Software and Algorithms	SDN	Blockchain, ICN, Virtualization Algorithms	Cipher Algorithms, Blockchain, Steganography	Call Admission Control (CAC)	–
	Machine Intelligence	Anomaly Detection	SDN	SDN	SDN	–
	Telecommunication Systems	–	5G, 6G	5G	5G/6G	5G, 6G

scalability, security, quality assurance, and energy efficiency. This comprehensive classification illustrates how each technology supports multi-dimensional optimization within IoT systems.

F. Novelty and Positioning of the Proposed Framework

While numerous studies have explored IoT performance optimization from isolated perspectives—such as microservice-based reliability, fault-tolerant mechanisms, lightweight security techniques, and device/network-level enhancements—these contributions remain largely fragmented across architectural layers and performance dimensions. Existing works typically address one layer at a time, or optimize a single performance requirement without acknowledging its interaction with other dimensions.

The proposed framework distinguishes itself from prior studies by offering a unified, multi-layer perspective that systematically integrates IoT architectural layers (device, network, support, and application) with multi-dimensional performance attributes (reliability, security, scalability, quality, and energy efficiency). Unlike previous reviews, which categorize solutions based solely on technology type or problem focus, the framework explicitly maps where each performance factor originates, how it propagates across layers, and which components or mechanisms influence it.

This holistic integration represents the primary novelty of the study. It enables a cross-layer understanding of IoT performance—an aspect not collectively addressed in existing literature—and provides a conceptual structure that researchers can use to analyze, compare, and design solutions more systematically. The accompanying taxonomy further reinforces this contribution by revealing performance-impacting components across layers and highlighting interdependencies that were previously treated in isolation.

IV. TAXONOMY OF IOT PERFORMANCE OPTIMIZATION COMPONENTS

Previous framework layers address the IoT multidimensional performance optimization problem and present various dimensions of requirements that are related to the IoT performance. This layer of the framework provides a taxonomy for the classification of various performance-impact components across multi-dimensional requirements and the main architectural layers of IoT systems. Furthermore, each component is analyzed based on the specific performance dimensions it targets, such as reliability, security, scalability, quality, and energy efficiency. The structured taxonomy and mapping of performance-impact components is presented in Table III. This mapping clearly explains how critical performance dimensions, scalability, quality, reliability, energy efficiency, and security are addressed across the IoT network layer architecture. The table taxonomy outlines the essential components within each layer (i.e., application, support, network, and device layers) and identifies the most relevant metrics for evaluating performance within those components. Besides, each architectural layer is decomposed into a key performance service or tool, allowing optimization-related performance components to be mapped with greater granularity.

V. PROMINENT SUGGESTED SOLUTIONS

Given the continuous evolution of IoT systems and their varying levels of complexity, exhaustively capturing and detailing all potential solutions is inherently difficult. However, this section seeks to synthesize the most salient solutions identified by researchers throughout the previously reviewed literature. The Table IV outlines these proposed approaches, categorizing them based on their contribution to critical performance requirements: Reliability, Security, Scalability, Quality, and Energy Efficiency. The following section discusses the key insights derived from these findings and highlights the implications for IoT performance optimization research.

VI. DISCUSSION AND KEY INSIGHTS

The findings of this study indicate that IoT performance research remains highly fragmented across architectural layers and performance dimensions. While numerous studies propose solutions targeting reliability, security, scalability, quality, or energy efficiency, these contributions are often isolated and optimized within a single layer or for a single performance requirement. This fragmentation limits the ability of researchers and practitioners to understand IoT performance holistically and to design solutions that address cross-layer interactions.

The literature review further shows a clear imbalance in research efforts. Most contributions focus on the network and device layers, particularly on routing, fault tolerance, cryptography, and lightweight service mechanisms. In contrast, the support and application layers receive less attention despite their growing role in enabling cloud–fog–edge intelligence, policy enforcement, orchestration, and application-level QoS. This gap highlights the need for more research

TABLE III. A TAXONOMY OF MULTI-DIMENSIONAL PERFORMANCE COMPONENTS ACROSS IOT ARCHITECTURE LAYERS

Layer	Impact Component, Tools, Service	Reliability	Scalability	Security	Quality	Energy Efficiency
Application Layer	Software Design and Engineering	Availability, Fault Tolerance, MTTR, MTTF	Response Time, Elasticity, Modularity, Throughput under Load	Integrity, Confidentiality, Authenticity, Privacy	Code Quality, Test Coverage, Reusability, Design Flexibility	Battery Life, Power Consumption
	Policies	Availability, Fault Tolerance	Policy Mgmt., Scalability, Elastic Demand Handling	Integrity, Confidentiality	Policy Completeness, Policy Failure Rate, Policy Rollback Time	Power Consumption per Operation
	Application Protocols	Availability, Fault Tolerance	Low Protocol Overhead, Latency Stability, Concurrent Support	Integrity, Confidentiality, Authenticity	Error Resilience, Latency for Data Delivery, Data Synchronization Quality	Energy Consumption during Idle and Active States
Support Layer	Resource Orchestrator	Fault-Tolerant, Redundancy	Resource Allocation, Task Scheduling, Concurrent Tasks Supported	Integrity, Confidentiality, Authentication	Resource Utilization Accuracy, Orchestration Decision Accuracy, SLA Compliance	Power Utilization Efficiency, Energy Management
	Cloud/Fog/Edge Integration	Availability, Fault Tolerance	Load Balancing, Elastic Resource Scaling	Integrity, Privacy	Interoperability, Data Consistency	Power Consumption for Data Processing
	Data (stored)	Availability, Fault Tolerance	Storage Access Scalability, Query Response Time	Integrity, Privacy, Confidentiality	Data Integrity, Latency of Data Access	Data Storage Power Efficiency
	Software/Hardware Components	Availability, Fault Tolerance	Component Modularity and Upgrade Flexibility, Resource Adaptability	Integrity, Authentication	Compatibility, Maintainability	Battery Efficiency
Network Layer	Routing Protocol	Availability, Fault Tolerance	Network Overhead, Convergence Time	Integrity, Confidentiality, Authentication	Packet Delivery Ratio (PDR), Latency, Stability	Energy Battery Life, Energy Consumption
	Internetworking Protocols	Availability, Fault Tolerance	Network Topology Scalability, Overhead, Interoperability	Integrity, Privacy, Authentication	Latency, Jitter, Channel Load, Packet Loss Rate	Transmission Energy Efficiency, Energy per Bit
	Flow Control	Availability, Fault-Tolerant, Error-Free Transmission	Load Handling Capacity	Integrity, Confidentiality	Buffer Size, Flow Stability, Admission Delay	Packet Processing Energy, Network Energy Efficiency
	Admission and Congestion Control Protocols	Availability, Fault Tolerance	Scalability with Flows, Queue Efficiency	Confidentiality, Authenticity	Queue Delay, QoS Maintenance, Rate of Packet Loss, Congestion Avoidance Efficiency	Power Consumption
	Addressing Protocols	Availability, Fault Tolerance	Address Allocation Efficiency, Address Space Utilization	Integrity, Confidentiality, Authentication	Resolution Delay, Address Uniqueness, Throughput	Power Consumption for Address Assignment
Device Layer	Communication and Signaling Protocols	Availability, Fault Tolerant	Protocol Overhead, Concurrent Device Support, Signal Range Expansion	Authentication, Confidentiality	Signal Strength Stability, Message Delivery Success Rate	Power Consumption for Transmission
	MAC and Access Control Protocol	Availability, Fault Tolerance	Access Contention Handling, Dynamic Node Joining Support	Integrity, Confidentiality, Authentication	MAC Delay, Packet Collision Rate	Energy Use for Access Control, Power Efficiency
	Error Correction and Detection	Availability, Fault Tolerance	Error Handling Scalability	Integrity, Privacy	Error Detection Rate, Detection Latency, Recovery Time from Errors	Power Consumption for Error Handling
	Data Collection and Buffering	Availability, Fault Tolerance	Buffer Scalability, Data Throughput under Load	Integrity, Privacy	Data Aggregation Efficiency, Collection Delay, Buffer Overflow Rate	Energy per Byte, Power during Data Collection
	Sensor Hardware and Software	Availability, Fault Tolerance	Device Resource Scalability, Firmware Update Flexibility	Authentication, Identification	Sensor Accuracy, Signal Quality	Energy Consumption per Sensor, Sleep Mode Power, Battery Life

into performance-aware service orchestration, data lifecycle management, and application-level adaptability.

The proposed multi-dimensional performance framework addresses these gaps by providing a unified structure that links IoT architectural layers with key performance dimensions and measurable metrics. Unlike existing studies that treat performance dimensions independently, the framework emphasizes their interdependence, illustrating how improvements at one layer (e.g., routing efficiency) may impact performance attributes at other layers (e.g., energy efficiency or QoS). The framework also clarifies the role of enabling technologies—such as virtualization, 5G/6G, blockchain, and IoT-specific protocols—in optimizing performance across the entire IoT ecosystem.

The taxonomy further contributes to the field by classifying performance-impact components across layers, revealing patterns and research priorities. For example, reliability-related components are heavily explored at the device and network layers, while quality-oriented solutions appear mostly at the application layer. Energy efficiency spans multiple layers, but most optimizations remain hardware-centric rather than system-wide. These patterns underscore the need for integrated, cross-layer optimization strategies.

Overall, the combined framework and taxonomy provide

TABLE IV. SUGGESTED SOLUTION APPROACHES

Solution approaches			Design requirements				
Techniques	**Class**	**Samples**	**Reliability**	**Security**	**Scalability**	**Quality**	**Energy efficiency**
Redundant design	Hardware redundancy	Triple modular redundancy	X	X		X	X
	Software redundancy	Multiversion programming					
	Information redundancy	Correction methods					
	Time redundancy	Same operation multiple times					
	Data redundancy	Keeping data in multiple locations					
ML tools	Classification	Naive Bayes	X	X		X	X
	Clustering	K-means					
	Regression	Linear regression					
Mathematical-based model	Deterministic	–	X	X	X	X	X
	Stochastic	–					
Numerical and computational method	Newton method	–	X	X	X	X	X
	Simpson rule	–					
	Euler method	–					
	Trapezoidal rule	–					
Statistical-based model	Parametric techniques	Gaussian, Non-Gaussian	X	X	X	X	X
	Non-parametric techniques	Kernel, Histogram					
Trust-based methods	Policy-based	–	X	X			X
	Recommendation-based	–					
	Reputation and feedback-based	–					
Data analysis	Descriptive	–			X	X	X
	Predictive	–					
	Prescriptive	–					
	Diagnostic	–					
Context-aware systems	Hardware context-awareness	–	X	X	X	X	X
	Software context-awareness	–					
Microservice architecture	Decomposition patterns	Sidecar	X	X	X	X	X
	Integration patterns	Aggregator					
	Observability patterns	Log aggregation					
	Cross-cutting concern patterns	Circuit breaker					
	Database patterns	Saga					
Optimization model	Linear optimization techniques	Integer, continuous, mixed-integer	X	X	X	X	X
	Nonlinear optimization techniques	–					
AI	Neural networks (NN)	–	X	X		X	X
	Fuzzy logic	–					
Swarm intelligence algorithms	Genetic algorithms (GA)	–	X				X
	Ant colony optimization (ACO)						
	Particle swarm optimization (PSO)						
	Differential evolution (DE)						
	Artificial bee colony (ABC)						
	Glowworm swarm optimization (GSO)						
	Cuckoo search algorithm (CSA)						
Ontology-based technique	Objective	–	X		X		X
	Subjective	–					

a foundation for future IoT performance research by 1) offering a structured view of performance-related components, 2) enabling systematic comparison of existing solutions, and 3) identifying gaps and opportunities for multi-layer optimization. This structured analytical view represents the primary contribution of this study and serves as a roadmap for designing next-generation IoT systems that balance reliability, security, energy, scalability, and quality in a unified manner.

VII. CONCLUSION

This paper successfully presented a comprehensive performance optimization framework designed for application across all layers of the IoT architecture. The framework serves as a critical foundation for identifying performance-related challenges and systematically guiding the development of tailored optimization solutions. While the overall design is holistic, a detailed taxonomy of existing optimization components was also introduced, synthesized from an extensive literature review. These components were classified according to five critical performance dimensions: reliability, security, scalability, quality assurance, and energy efficiency. Each dimension was analyzed by detailing its unique challenges and the specific metrics required for practical evaluation.

Additionally, the paper highlighted the vital role of enabling technologies—spanning hardware, software, machine intelligence, and telecommunication systems—in supporting multi-dimensional performance optimization. The integration of these technologies is essential for realizing scalable, secure, and efficient IoT environments. The conceptual model, performance taxonomy, and technological mapping developed in this paper collectively lay the groundwork for future research and methodical system design.

Acknowledgment

This work is funded by the Ongoing Research Funding program, (ORF-2025-1415), King Saud University, Riyadh, Saudi Arabia.

References

[1] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and iot in smart transportation," *Future Internet*, vol. 11, no. 4, p. 94, 2019.

[2] M. Swan, "Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0," *Journal of Sensor and Actuator networks*, vol. 1, no. 3, pp. 217–253, 2012.

[3] D. Evans, "The internet of things how the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, pp. 1–11, 2011.

[4] S. Rudrakar and P. Rughani, "Iot based agriculture (ag-iot): A detailed study on architecture, security and forensics," *Information Processing in Agriculture*, 2023.

[5] A. Rayes and S. Salam, "The things in iot: Sensors and actuators," in *Internet of Things From Hype to Reality*. Springer, 2022, pp. 63–82.

[6] N. K. Saini, "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)*. IEEE, 2016, pp. 411–414.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[8] S. J. Moore, C. D. Nugent, S. Zhang, and I. Cleland, "Iot reliability: a review leading to 5 key research directions," *CCF Transactions on Pervasive Computing and Interaction*, vol. 2, no. 3, pp. 147–163, 2020.

[9] M. A. da Cruz, J. J. Rodrigues, A. K. Sangaiah, J. Al-Muhtadi, and V. Korotaev, "Performance evaluation of iot middleware," *Journal of Network and Computer Applications*, vol. 109, pp. 53–65, 2018.

[10] Z. Menter, W. Z. Tee, and R. Dave, "Application of machine learning-based pattern recognition in iot devices," in *Proceedings of International Conference on Communication and Computational Technologies*. Springer, 2021, pp. 669–689.

[11] C. Santana, L. Andrade, F. C. Delicato, and C. Prazeres, "Increasing the availability of iot applications with reactive microservices," *Service Oriented Computing and Applications*, vol. 15, no. 2, pp. 109–126, 2021.

[12] L. M. e. Martins, F. L. d. C. Filho, R. T. d. S. Júnior, W. F. Giozza, and J. P. C. da Costa, "Increasing the dependability of iot middleware with cloud computing and microservices," in *Companion Proceedings of the10th International Conference on Utility and Cloud Computing*, 2017, pp. 203–208.

[13] G. Aquino, R. Queiroz, G. Merrett, and B. Al-Hashimi, "The circuit breaker pattern targeted to future iot applications," in *International Conference on Service-Oriented Computing*. Springer, 2019, pp. 390–396.

[14] N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "Towards fault tolerant fog computing for iot-based smart city applications," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2019, pp. 0752–0757.

[15] R. K. Behera, K. H. K. Reddy, and D. S. Roy, "Reliability modelling of service oriented internet of things," in *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)*. IEEE, 2015, pp. 1–6.

[16] T. N. Gia, A.-M. Rahmani, T. Westerlund, P. Liljeberg, and H. Tenhunen, "Fault tolerant and scalable iot-based architecture for health monitoring," in *2015 IEEE Sensors Applications Symposium (SAS)*. IEEE, 2015, pp. 1–6.

[17] M. Z. Hasan and F. Al-Turjman, "Optimizing multipath routing with guaranteed fault tolerance in internet of things," *IEEE Sensors Journal*, vol. 17, no. 19, pp. 6463–6473, 2017.

[18] A. Mavrogiorgou, A. Kiourtis, C. Symvoulidis, and D. Kyriazis, "Capturing the reliability of unknown devices in the iot world," in *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*. IEEE, 2018, pp. 62–69.

[19] T. T. Zin, P. Tin, and H. Hama, "Reliability and availability measures for internet of things consumer world perspectives," in *2016 IEEE 5th Global Conference on Consumer Electronics*. IEEE, 2016, pp. 1–2.

[20] K. Periyasamy, V. Alagar, and K. Wan, "Dependable design for elderly health care," in *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 2017, pp. 803–806.

[21] A. Celesti, L. Carnevale, A. Galletta, M. Fazio, and M. Villari, "A watchdog service making container-based micro-services reliable in iot clouds," in *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, 2017, pp. 372–378.

[22] A. Power and G. Kotonya, "A microservices architecture for reactive and proactive fault tolerance in iot systems," in *2018 IEEE 19th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2018, pp. 588–599.

[23] I. Kopestenski and P. Van Roy, "Erlang as an enabling technology for resilient general-purpose applications on edge iot networks," in *Proceedings of the 18th ACM SIGPLAN International Workshop on Erlang*, 2019, pp. 1–12.

[24] P. Vedavalli and C. Deepak, "Enhancing reliability and fault tolerance in iot," in *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)*. IEEE, 2020, pp. 1–6.

[25] W.-T. Lee and P.-J. Law, "A case study in applying security design patterns for iot software system," in *2017 international conference on applied system innovation (ICASI)*. IEEE, 2017, pp. 1162–1165.

[26] E. B. Fernandez, H. Washizaki, N. Yoshioka, and T. Okubo, "The design of secure iot applications using patterns: State of the art and directions for research," *Internet of Things*, vol. 15, p. 100408, 2021.

[27] I. Ali and M. Asif, "Applying security patterns for authorization of users in iot based applications," in *2018 International Conference on Engineering and Emerging Technologies (ICEET)*. IEEE, 2018, pp. 1–5.

[28] Z. B. Celik, G. Tan, and P. D. McDaniel, "Iotguard: Dynamic enforcement of security and safety policy in commodity iot." in *NDSS*, 2019.

[29] I. Cvitić, D. Peraković, M. Periša, and B. Gupta, "Ensemble machine learning approach for classification of iot devices in smart home," *International Journal of Machine Learning and Cybernetics*, vol. 12, no. 11, pp. 3179–3202, 2021.

[30] N. Paul, W. B. Tesfay, D.-K. Kipker, M. Stelter, and S. Pape, "Assessing privacy policies of internet of things services," in *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 2018, pp. 156–169.

[31] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for iot based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139 244–139 254, 2020.

[32] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure mqtt for internet of things (iot)," in *2015 fifth international conference on communication systems and network technologies*. IEEE, 2015, pp. 746–751.

[33] D. Nagothu, R. Xu, S. Y. Nikouei, and Y. Chen, "A microservice-enabled architecture for smart surveillance using blockchain technology," in *2018 IEEE international smart cities conference (ISC2)*. IEEE, 2018, pp. 1–4.

[34] A. A. Omala, A. S. Mbandu, K. D. Mutiria, C. Jin, and F. Li, "Provably secure heterogeneous access control scheme for wireless body area network," *Journal of Medical Systems*, vol. 42, no. 6, pp. 1–14, 2018.

[35] A. Strielkina, V. Kharchenko, and D. Uzun, "Availability models for healthcare iot systems: Classification and research considering attacks on vulnerabilities," in *2018 IEEE 9th international conference on dependable systems, services and technologies (DESSERT)*. IEEE, 2018, pp. 58–62.

[36] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "Iot-based big data secure management in the fog over a 6g wireless network," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5164–5171, 2021.

[37] C. Zhang, Y. Miao, Q. Xie, Y. Guo, H. Du, and X. Jia, “Privacy-preserving deduplication of sensor compressed data in distributed fog computing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 12, pp. 4176–4191, 2022.

[38] W. Jerbi, A. Guermazi, and H. Trabelsi, “A secure routing protocol in heterogeneous networks for internet of things,” in *2020 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 2020, pp. 571–576.

[39] ——, “Design and deployment of a security protocol to provide authentication services for connected objects,” in *Proceedings of the 10th Euro-American Conference on Telematics and Information Systems*, 2020, pp. 1–6.

[40] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, “Split: A secure and scalable rpl routing protocol for internet of things,” in *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2018, pp. 1–8.

[41] ——, “Attestation-enabled secure and scalable routing protocol for iot networks,” *Ad Hoc Networks*, vol. 98, p. 102054, 2020.

[42] K. Haseeb, A. Almogren, N. Islam, I. Ud Din, and Z. Jan, “An energy-efficient and secure routing protocol for intrusion avoidance in iot-based wsn,” *Energies*, vol. 12, no. 21, p. 4174, 2019.

[43] Y. He, G. Han, H. Wang, J. A. Ansere, and W. Zhang, “A sector-based random routing scheme for protecting the source location privacy in wsns for the internet of things,” *Future Generation Computer Systems*, vol. 96, pp. 438–448, 2019.

[44] K. Quist-Aphetsi and M. C. Xenya, “Node to node secure data communication for iot devices using diffie-hellman, aes, and md5 cryptographic schemes,” in *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*. IEEE, 2019, pp. 88–92.

[45] D. Dinculeană and X. Cheng, “Vulnerabilities and limitations of mqtt protocol used between iot devices,” *Applied Sciences*, vol. 9, no. 5, p. 848, 2019.

[46] A. Cohen, A. Cohen, and O. Gurewitz, “Secured data gathering protocol for iot networks,” in *International Symposium on Cyber Security Cryptography and Machine Learning*. Springer, 2018, pp. 129–143.

[47] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, “Secured data collection with hardware-based ciphers for iot-based healthcare,” *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 410–420, 2018.

[48] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, “Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review,” *Journal of Network and Computer Applications*, vol. 190, p. 103118, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804521001375

[49] A. Razzaq, “A systematic review on software architectures for iot systems and future direction to the adoption of microservices architecture,” *SN Computer Science*, vol. 1, no. 6, pp. 1–30, 2020.

[50] A. El-Mougy, I. Al-Shiab, and M. Ibnkahla, “Scalable personalized iot networks,” *Proceedings of the IEEE*, vol. 107, no. 4, pp. 695–710, 2019.

[51] I. Zyrianoff, F. Borelli, G. Biondi, A. Heideker, and C. Kamienski, “Scalability of real-time iot-based applications for smart cities,” in *2018 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2018, pp. 00 688–00 693.

[52] S. Busanelli, S. Cirani, L. Melegari, M. Picone, M. Rosa, and L. Veltri, “A sidecar object for the optimized communication between edge and cloud in internet of things applications,” *Future Internet*, vol. 11, no. 7, p. 145, 2019.

[53] S. K. Mishra and A. Sarkar, “Service-oriented architecture for internet of things: a semantic approach,” *Journal of King Saud University-Computer and Information Sciences*, 2021.

[54] H. Guo, J. Ren, D. Zhang, Y. Zhang, and J. Hu, “A scalable and manageable iot architecture based on transparent computing,” *Journal of Parallel and Distributed Computing*, vol. 118, pp. 5–13, 2018.

[55] S. Verma and A. Bala, “Auto-scaling techniques for iot-based cloud applications: a review,” *Cluster Computing*, vol. 24, no. 3, pp. 2425–2459, 2021.

[56] B. Sonkoly, D. Haja, B. Németh, M. Szalay, J. Czentye, R. Szabó, R. Ullah, B.-S. Kim, and L. Toka, “Scalable edge cloud platforms for iot services,” *Journal of Network and Computer Applications*, vol. 170, p. 102785, 2020.

[57] E. Rojas, H. Hosseini, C. Gomez, D. Carrascal, and J. R. Cotrim, “Outperforming rpl with scalable routing based on meaningful mac addressing,” *Ad Hoc Networks*, vol. 114, p. 102433, 2021.

[58] F. Li, S. Nastic, and S. Dustdar, “Data quality observation in pervasive environments,” in *2012 IEEE 15th International Conference on Computational Science and Engineering*. IEEE, 2012, pp. 602–609.

[59] E. Al-Masri, “Qos-aware iiot microservices architecture,” in *2018 IEEE International Conference on Industrial Internet (ICII)*. IEEE, 2018, pp. 171–172.

[60] G. White, V. Nallur, and S. Clarke, “Quality of service approaches in iot: A systematic mapping,” *Journal of Systems and Software*, vol. 132, pp. 186–203, 2017.

[61] M. Singh and G. Baranwal, “Quality of service (qos) in internet of things,” in *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*. IEEE, 2018, pp. 1–6.

[62] M. Taneja, N. Jalodia, J. Byabazaire, A. Davy, and C. Olariu, “Smartherd management: A microservices-based fog computing–assisted iot platform towards data-driven smart dairy farming,” *Software: practice and experience*, vol. 49, no. 7, pp. 1055–1078, 2019.

[63] M. Quwaider and Y. Shatnawi, “Congestion control model for securing internet of things data flow,” *Ad Hoc Networks*, vol. 106, p. 102160, 2020.

[64] L. Yao, J.-Y. Shen, and W. H. Lim, “Real-time energy management optimization for smart household,” in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2016, pp. 20–26.

[65] S. Kim, C. Kim, and J. Kim, “Reliable smart energy iot-cloud service operation with container orchestration,” in *2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*. IEEE, 2017, pp. 378–381.

[66] N.-T. Dinh and Y. Kim, “An efficient on-demand latency guaranteed interactive model for sensor-cloud,” *IEEE Access*, vol. 6, pp. 68 596–68 611, 2018.

[67] Z. T. Al-Azez, A. Q. Lawey, T. E. El-Gorashi, and J. M. Elmirghani, “Energy efficient iot virtualization framework with passive optical access networks,” in *2016 18th International Conference on Transparent Optical Networks (ICTON)*. IEEE, 2016, pp. 1–4.

[68] I. S. M. Isa, M. O. Musa, T. E. El-Gorashi, A. Q. Lawey, and J. M. Elmirghani, “Energy efficiency of fog computing health monitoring applications,” in *2018 20th International Conference on Transparent Optical Networks (ICTON)*. IEEE, 2018, pp. 1–5.

[69] H. Q. Al-Shammari, A. Lawey, T. El-Gorashi, and J. M. Elmirghani, “Energy efficient service embedding in iot networks,” in *2018 27th Wireless and Optical Communication Conference (WOCC)*. IEEE, 2018, pp. 1–5.

[70] N. Kaur and S. K. Sood, “An energy-efficient architecture for the internet of things (iot),” *IEEE Systems Journal*, vol. 11, no. 2, pp. 796–805, 2015.

[71] H. M. Al-Kadhim and H. S. Al-Raweshidy, “Energy efficient and reliable transport of data in cloud-based iot,” *IEEE Access*, vol. 7, pp. 64 641–64 650, 2019.

[72] L. Lyu, C. Chen, S. Zhu, and X. Guan, “5g enabled codesign of energy-efficient transmission and estimation for industrial iot systems,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2690–2704, 2018.

[73] Y. Wang, W. Yang, X. Shang, J. Hu, Y. Huang, and Y. Cai, “Energy-efficient secure transmission for wireless powered internet of things with multiple power beacons,” *IEEE Access*, vol. 6, pp. 75 086–75 098, 2018.

[74] A. Slalmi, H. Kharraz, R. Saadane, C. Hasna, A. Chehri, and G. Jeon, “Energy efficiency proposal for iot call admission control in 5g network,” in *2019 15th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*. IEEE, 2019, pp. 396–403.

[75] D. Purkovic, M. Hönsch, and T. R. M. K. Meyer, "An energy efficient communication protocol for low power, energy harvesting sensor modules," *IEEE Sensors Journal*, vol. 19, no. 2, pp. 701–714, 2018.

[76] S. Abbasian Dehkordi, K. Farajzadeh, J. Rezazadeh, R. Farahbakhsh, K. Sandrasegaran, and M. Abbasian Dehkordi, "A survey on data aggregation techniques in iot sensor networks," *Wireless Networks*, vol. 26, no. 2, pp. 1243–1263, February 2020. [Online]. Available: https://doi.org/10.1007/s11276-019-02142-z

[77] E. Bradley, *Reliability engineering: a life cycle approach*. Crc Press, 2016.

[78] S. J. Pokorni, "Reliability and availability of the internet of things," *Vojnotehnički glasnik*, vol. 67, no. 3, pp. 588–600, 2019.

[79] R. C. Fries, *Reliable design of medical devices*. CRC Press, 2005.

[80] S. J. Moore, C. D. Nugent, S. Zhang, and I. Cleland, "Iot reliability: a review leading to 5 key research directions," *CCF Transactions on Pervasive Computing and Interaction*, vol. 2, no. 3, pp. 147–163, 2020.

[81] S. J. Pokorni, "Reliability and availability of the internet of things," *Vojnotehnički glasnik*, vol. 67, no. 3, pp. 588–600, 2019.

[82] F. M. R. Junior and C. A. Kamienski, "A survey on trustworthiness for the internet of things," *IEEE Access*, vol. 9, pp. 42 493–42 514, 2021.

[83] S. Sarkar, "Internet of things—robustness and reliability," in *Internet of Things*. Elsevier, 2016, pp. 201–218.

[84] S. V. Kolla, "Machine learning and its application in iot," 2021.

[85] L. E. Kane, J. J. Chen, R. Thomas, V. Liu, and M. Mckague, "Security and performance in iot: A balancing act," *IEEE access*, vol. 8, pp. 121 969–121 986, 2020.

[86] A. H. M. Aman, E. Yadegaridehkordi, Z. S. Attarbashi, R. Hassan, and Y.-J. Park, "A survey on trend and classification of internet of things reviews," *Ieee Access*, vol. 8, pp. 111 763–111 782, 2020.

[87] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of things (iot): A vision, architectural elements, and security issues," in *2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017, pp. 492–496.

[88] R. Hu, Z. Yan, W. Ding, and L. T. Yang, "A survey on data provenance in iot," *World Wide Web*, vol. 23, no. 2, pp. 1441–1463, 2020.

[89] F. Zafar, A. Khan, S. Suhail, I. Ahmed, K. Hameed, H. M. Khan, F. Jabeen, and A. Anjum, "Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes," *Journal of network and computer applications*, vol. 94, pp. 50–68, 2017.

[90] T. Ulz, T. Pieber, C. Steger, R. Matischek, and H. Bock, "Towards trustworthy data in networked control systems: A hardware-based approach," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2017, pp. 1–8.

[91] I. Belkacem, S. Nait-Bahloul, and D. Sauveron, "Enhancing dependability through profiling in the collaborative internet of things," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 2983–3007, 2019.

[92] A. B. Bondi, "Characteristics of scalability and their impact on performance," in *Proceedings of the 2nd international workshop on Software and performance*, 2000, pp. 195–203.

[93] I. Zyrianoff, F. Borelli, G. Biondi, A. Heideker, and C. Kamienski, "Scalability of real-time iot-based applications for smart cities," in *2018 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2018, pp. 00 688–00 693.

[94] A. Gupta, R. Christie, and R. Manjula, "Scalability in internet of things: features, techniques and research challenges," *Int. J. Comput. Intell. Res*, vol. 13, no. 7, pp. 1617–1627, 2017.

[95] A. Javed, A. Malhi, T. Kinnunen, and K. Främling, "Scalable iot platform for heterogeneous devices in smart environments," *IEEE Access*, vol. 8, pp. 211 973–211 985, 2020.

[96] A. Al-Said Ahmad and P. Andras, "Scalability analysis comparisons of cloud-based software services," *Journal of Cloud Computing*, vol. 8, no. 1, pp. 1–17, 2019.

[97] K. Subash, D. J. Ramya, and L. Arockiam, "Quality of service in the internet of things (iot)–a survey," *TIRUCHIRAPPALLI-620 002, TAMIL NADU, INDIA*, 2019.

[98] B. S. Ahmed, M. Bures, K. Frajtak, and T. Cerny, "Aspects of quality in internet of things (iot) solutions: A systematic mapping study," *IEEE Access*, vol. 7, pp. 13 758–13 780, 2019.

[99] E. Cero, J. Baraković Husić, and S. Baraković, "Iot's tiny steps towards 5g: Telco's perspective," *Symmetry*, vol. 9, no. 10, p. 213, 2017.

[100] E. Borgia, "The internet of things vision: Key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[101] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers, 2013.

[102] O. Vermesan, P. Friess *et al.*, *Internet of things-from research and innovation to market deployment*. River publishers Aalborg, 2014, vol. 29.