

Non-Functional Requirement (NFR) Characteristics for Cloud-Based IoT Systems: A Systematic Literature Review

Nor Faradila Kolan^{1*}, Fazlina Mohd Ali²,

Elankovan A. Sundararajan³, Marizuana Mat Daud⁴, Siti Nur'asyiqin Ismael⁵

Faculty of Information Science and Technology (FTSM), Universiti Kebangsaan Malaysia (UKM), Selangor, Malaysia^{1, 2, 3}

Institute of IR 4.0, Universiti Kebangsaan Malaysia, Bangi, Malaysia (UKM), Selangor, Malaysia⁴

Azman Hashim International Business School, Universiti Teknologi Malaysia⁵

Abstract—The rapid development and increasing integration of the Internet of Things (IoT) and cloud computing can improve a system's ability to process big data in real time. These technologies complement each other. A cloud-based IoT system is more complex and presents new challenges in requirements engineering, especially for non-functional requirements (NFRs). Additionally, NFRs play a significant role in determining software quality and user satisfaction. Thus, gaps in requirements specification studies increase development costs, rework, and the risk of project failure. Failure to identify NFRs systematically and manage them through effective governance leads to ambiguous requirements and unmet user requirements. Therefore, this systematic literature review (SLR) aims to identify and classify the main NFR characteristics of cloud-based IoT systems. This study adopted the PRISMA approach to identify and select literature. A total of 180 studies were initially identified from four main online databases, of which 21 final selected studies from 2017 to mid-2026 met the inclusion criteria. The findings were grouped into nine NFR characteristics relevant to cloud-based IoT system development, namely Performance Efficiency, Compatibility, Interaction Capability, Reliability, Security, Maintainability, Flexibility, Safety, and External Requirements. The main contribution of this study is to identify and classify NFR challenges, significant NFR characteristics, and publication trends for cloud-based IoT system development. This SLR will be valuable to academics and researchers in this field.

Keywords—Non-functional requirement; software engineering; requirement engineering; Internet of Things; cloud computing

I. INTRODUCTION

Emerging technology-driven system development is evolving through artificial intelligence, cloud computing, Internet of Things, and blockchain [1]. The development of IoT systems is progressing rapidly, with more organizations increasingly implementing IoT technologies in their systems and operations.

This study was supported by the National University of Malaysia (UKM) www.ftsm.ukm.my/softam.

Moreover, efficient technology supports smart governance by processing data and enabling decision-making in the digital era. One advantage of emerging technology is that it provides the best software for security and IoT network protection [2]. In addition, some past studies have stated that the number of

devices has increased as expected, with 22 billion in 2018 [3], 38.6 billion in 2025 [4], and is expected to reach 50 billion in the year 2030 [3], [4], as shown in Fig. 1.

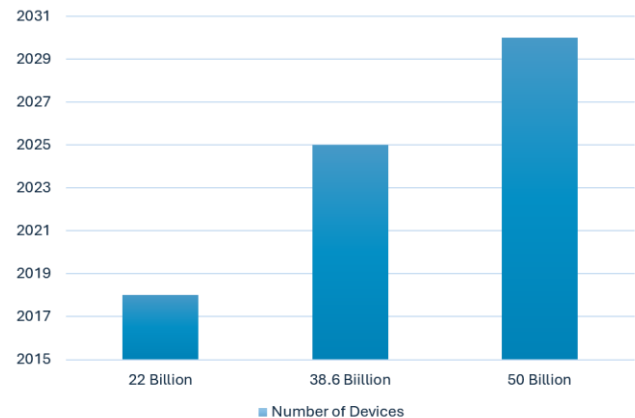


Fig. 1. Number of devices in the Internet of Things.

The graph in Fig. 1 reveals that IoT device connectivity has increased as expected and will continue to grow due to big data adoption. This fact has been supported by International Data Corporation (IDC) report in 2025 that the global number of connected devices was projected to reach about 55.7 billion, of which around 75% will be connected to IoT platforms [5] and also devices connected to the network will produce about 163 zettabytes (ZB) of data [6]. Among digital transformation components, IoT has been used in smart governance, smart health, smart industry, smart transportation, and more. IoT is defined as a complete object with sensors that drives a complete system with an interface connected to the Internet for data exchange [7]. In addition, IoT is the foundation for various smart systems such as smart cities, smart healthcare, and intelligent transport systems [7], [8]. As the data grows tremendously the cloud platforms become crucial enabler to store all the huge numbers of data safely.

Cloud computing is well known as a provider of numerous slices such as servers, storage, databases, networking, software, and analytics to users on demand [9]. However, weaknesses in cloud computing, such as limited infrastructure and networks, can reduce performance [10]. In addition, cloud computing has

*Corresponding author.

three main service models, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [11]. Cloud computing can be implemented in real-world industries through three implementations: public cloud, private cloud, and hybrid cloud [12]. In general, most previous studies agree that using cloud systems can overcome resource constraints on IoT devices, such as limited processing capacity, small storage, and the inability to handle large-scale data automatically [13]. The data management revolution in cloud computing provides flexible and scalable storage solutions based on user requirements [14]. IoT can benefit from the cloud by integrating and improving existing IoT processes [15].

IoT and cloud integration enable IoT devices to connect with the infrastructure for data storage, data analytics, and service delivery [16]. Cloud-IoT integration makes IoT devices data sources, while cloud-based systems are used to process and analyze data to produce real-time data [17]. An integrated requirements engineering (RE) process plays a vital role in developing cloud-based IoT systems. Large-scale system development involves many requirements, and determining success is crucial [18].

RE is the process of understanding user requirements, identifying, evaluating solutions, verifying specifications, and managing requirements throughout system development [19]. On the other hand, RE aims to ensure that "what the system should do" and "how the system should operate" are clearly defined from the beginning of system development to reduce misinterpretations, the risk of failure, and high-cost changes in the next phase [20]. According to [21], a system is generally usable, effective, and free from faults for the user; the user's requirements must be considered when determining the factors that affect the quality of the system. In the RE context, requirements are divided into two parts: functional requirements (FR) and non-functional requirements (NFR), as shown in Fig. 2. However, FR defines what the system does, while NFR determines how the system functions based on user requirements.

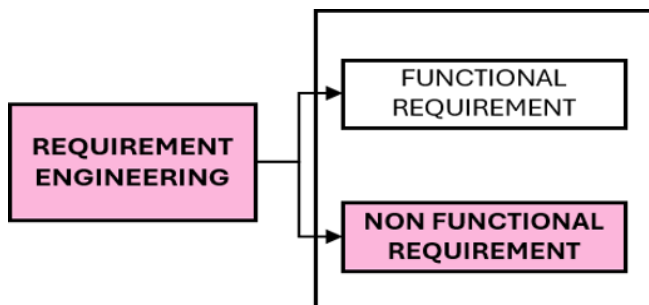


Fig. 2. Requirement engineering.

According to previous studies, NFR is known as a software quality standard requirement, while FR can be defined as a service, function, or behavior that a system can provide [22]. These functions should be concurrent and must be present in any type of system development, whether it is an IoT system or a conventional system. There are many emerging technology-driven developments in the system. It consists of NFRs and FR driven by emerging technology.

NFRs remain critical in software engineering for determining the quality of the system produced. Thus, the security and reliability of NFR technology can increase rapidly [1]. Previous studies show that industry practice prioritizes technological advancement security and efficiency are often treated as secondary outcomes [23]. With the availability of international references such as ISO, few changes have occurred in the specialization of software quality as a product, including quality models [24]. To ensure NFRs in cloud-based IoT, specific NFR characteristics are needed to identify and guide the characteristics that influence proper and effective performance. In addition, user satisfaction with NFR remains unexplored [24]. NFRs are often incomprehensible to end users, as they involve technical aspects such as speed data, network accessibility, and network performance.

Thus as this, cloud-based IoT systems are rapidly growing in use, and the characteristics of FR and NFR remain underexplored. FR is system-specific and difficult to identify as a main characteristic because it depends on the project scope, whereas NFR generalizes characteristics that can be applied to every project in a cloud-based IoT system. Although numerous studies have theoretically explored NFR, few researchers have consolidated the prominent NFR in their studies. This SLR explores NFR characteristics for cloud-based IoT systems to benefit future research and the development of cloud-based IoT systems.

II. RELATED WORK

Most previous studies examined NFR and FR simultaneously in the context of requirements specification on FR-oriented modeling, validation, and architectural design [25]. FR helps understand IoT system requirements, and the focus is more on system operational requirements rather than on quality. In contrast, some recent studies have shifted the focus to NFRs by emphasizing various aspects of system quality. Authors in [26] examine privacy and security issues in the Cloud of Things (CoT), while [27] focuses on Quality of Service (QoS) for cloud-assisted middleware-based IoT and other applications. Additionally, [27] evaluated NFR in the context of middleware and edge computing, showing that characteristics such as performance, reliability, and scalability are increasingly recognized as main characteristics in the development of modern systems. Authors in [28] examine how the design is suited to collect NFRs, [29] identify NFRs from FR characteristics using the standard ISO/IEC25023, and [30] propose a new approach to identifying NFRs.

Although research on NFRs continues to grow, previous studies have generally addressed different aspects of NFRs separately. For example, [31] focuses on performance and timeliness, while [32] examines API quality. Study [33] proposes an NFR measurement model based on FURPS, whereas [34] presents an NFR framework for business systems. Other studies have explored the prioritisation of NFRs [35] and their automatic classification [36]. These contributions provide useful insights into NFR identification, measurement, and management. However, they address different research objectives and application contexts, and their findings do not necessarily represent the NFR characteristics of cloud-based IoT systems specifically. This makes it important to examine the

evidence available in studies that fall within the scope of cloud-based IoT, rather than assuming that findings from general NFR research can be directly applied to this context.

Other approaches have been proposed to support NFR management, including use case modelling [37], model-driven approaches [38], and the use of large language models (LLMs) for NFR elicitation [39]. These approaches offer different ways to identify and manage quality requirements during system development. However, their applicability to cloud-based IoT systems needs to be considered in relation to the specific challenges of integrating IoT devices with cloud infrastructure and services. The relationship between functional requirements (FRs) and NFRs also remains important, as system functions alone do not fully describe the quality expected from a system. As discussed in [32], both types of requirements need to be considered during development. In addition, the guidelines presented in [40] and [41] highlight the importance of addressing requirements carefully in specific application contexts, including Smart Campus development. Taken together, these studies provide useful foundations for NFR engineering, but further examination is needed to understand how NFR characteristics are addressed specifically in cloud-based IoT systems.

The literature reviewed highlights the need for a clearer understanding of NFR characteristics in cloud-based IoT systems. Although previous studies have examined various aspects of NFRs, their findings cover different application contexts and individual quality concerns. As a result, it remains difficult to determine how these characteristics are addressed collectively within the cloud-based IoT context. This gap provides the motivation for the present systematic literature review, which examines the selected studies to identify and classify the NFR characteristics reported in cloud-based IoT systems. Fig. 3 illustrates the classification of previous studies according to their focus on functional requirements (FRs), non-functional requirements (NFRs), or both. This classification provides a broader view of how requirements have been addressed in previous research and helps establish the context for the present review.

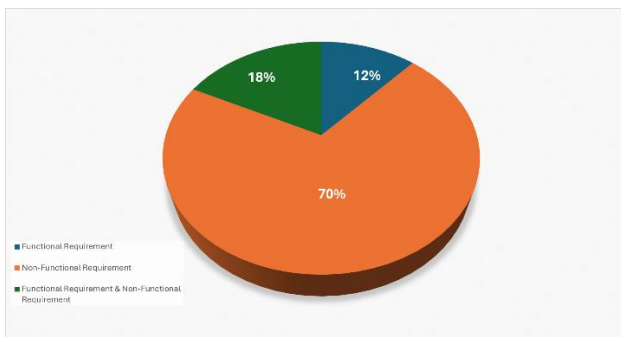


Fig. 3. Requirements classification.

This gap is important to be addressed because failing to identify and manage NFRs systematically can affect system performance entirely. Consequently, it can increase development costs and the risk of project failure [17]. Therefore, this gap motivated the present SLR to identify comprehensive NFR characteristics for cloud-based IoT systems.

III. RESEARCH METHODOLOGY

This SLR process consists of three phases: planning, conducting, and reporting [42]. To ensure transparency in selecting and reporting studies, this study used the PRISMA guidelines [43]. The SLR process is shown in Table I.

TABLE I. SYSTEMATIC LITERATURE REVIEW PHASE

Phases	Steps
Planning	Research Question Data Resources Search String Strategy Inclusion and Exclusion Criteria
Conducting	Primary Study Selection Data Inclusion and Exclusion
Reporting	Synthesis Report

A. Planning Phase

1) *Research question*: This study was designed to answer the following questions:

a) *RQ1*: What are the key challenges reported in cloud-based IoT systems that are relevant to non-functional requirements (NFR)?

b) *RQ2*: What are the main characteristics of non-functional requirements (NFR) identified in cloud-based IoT systems?

c) *RQ3*: What are the publication trends in cloud-based IoT studies over the years?

2) *Data resources*: A Literature search was conducted using a database that included:

a) Web of Science

b) IEEE Xplore

c) Scopus

d) ScienceDirect

3) *Search string strategy*: The study used online resources and searched in academic databases. To combine keywords into the search, use the Boolean operators “AND” and “OR” followed by keywords:

TABLE II. KEYWORDS

Databases	Keywords
IEEE Xplore	("non-functional requirements" OR system development" AND "cloud-based IoT" AND "software requirement" AND "requirement engineering")
Web of Science (WoS)	("non-functional requirements" OR system development" AND "cloud-based IoT")
Scopus	("non-functional requirements" AND "cloud-based IoT" OR "NFR" OR "cloudIoT")
Science Direct	("non-functional requirements" AND "cloud based IoT" OR "NFR" OR "cloudIoT")

4) *Inclusion and exclusion criteria*: In the selection of data inclusion, this study used measurements of previous studies [62] as a guide as follows:

a) Written in English.

b) Published between 2017 and mid-2026.

c) Articles relevant to the research objectives, including studies on IoT–cloud integration, NFR-related challenges, NFR characteristics, and other issues in the development and operation of cloud-based IoT systems.

5) On the other hand, the exclusion criteria included the following conditions:

- a) Repetitive (redundant) articles.
- b) Articles written in languages other than English.
- c) Published outside the study period from 2017 to mid-2026.

B. Conducting Phase

1) *Primary study selection:* The data inclusion and exclusion criteria included peer-reviewed journal and conference articles, focusing on NFR in the context of IoT and cloud computing. Articles not directly related to or outside the target period are removed through the exclusion process.

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) is a guideline for reporting in systematic reviews that helps identify, select, appraise, and synthesize studies [44]. Thus, it helps researchers report the flow of studies comprehensively and transparently. In addition, PRISMA also has a PRISMA flow diagram, which is used for mapping the total reading material identified, filtered, and excluded with justifications to improve transparency. Fig. 4 shows the PRISMA Systematic Literature Review of this study.

2) Data inclusion and exclusion

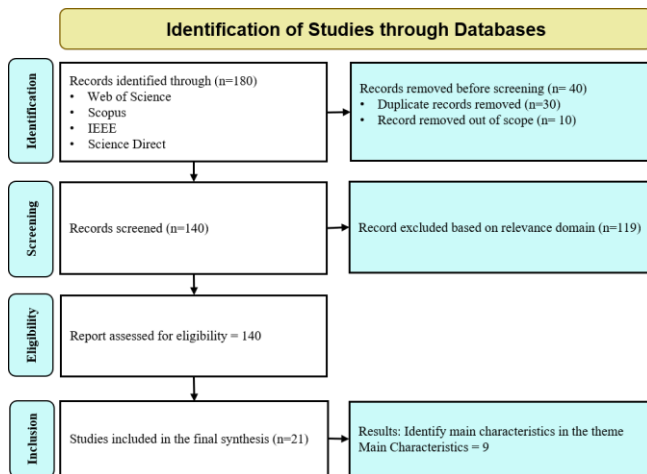


Fig. 4. PRISMA-based paper selection.

3) *Data extraction and NFR classification:* The 21 selected studies varied in the extent of explicit engagement with NFRs. While some studies directly addressed software quality attributes or NFR-related topics, others examined technical issues, challenges, and quality mechanisms of cloud-based IoT systems, such as performance efficiency, security, reliability, scalability, and interoperability. Therefore, the selected studies were not assumed to adopt a common NFR classification or to explicitly use all nine characteristics established in this review. Instead, the relevant findings reported in each study were examined and mapped to the nine NFR characteristics based on

their conceptual meaning and the operational definitions adopted in this research.

A characteristic was assigned to a study only when its reported content provided sufficient supporting evidence. This approach enabled the review to synthesise NFR-related evidence across studies with different research emphases while maintaining traceability between the classification and the original findings. The result represents the classification developed in this review rather than a claim that all selected studies used the same NFR framework.

C. Reporting Phase

1) *Synthesis reporting:* Overall, the synthesis reporting phase aims to report findings from selected studies and present them systematically to produce a comprehensive summary.

IV. FINDINGS AND DISCUSSION

This section presents findings from 21 selected studies on NFR in system development. Each main characteristic is examined in relation to the three research questions (RQ1–RQ3), and each question is discussed in sub-sections.

A. RQ1: What Are the Key Challenges Reported in Cloud-Based IoT Systems that Are Relevant to Non-Functional Requirements (NFR)?

This study explores the challenges arising from unclear NFRs in cloud-based IoT system development. Existing research identifies similar challenges across the literature, suggesting the need for a comprehensive set of NFRs that addresses them holistically and supports high-quality development of cloud-based IoT systems.

The issues identified in RQ1 reveal challenges that lead into issues related to the development of cloud-based IoT systems. Fig. 5 illustrates five main challenge themes.

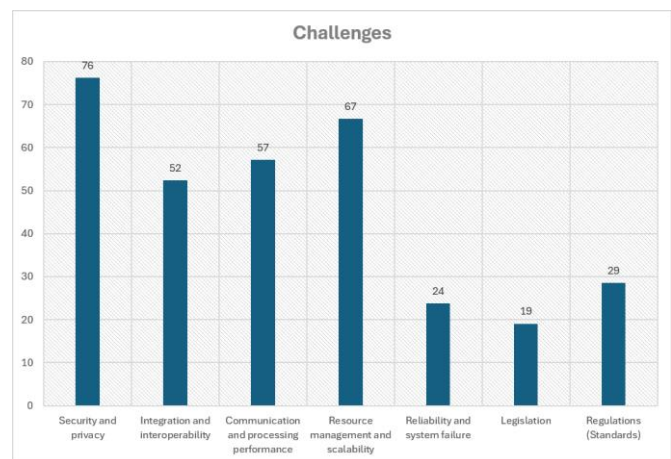


Fig. 5. Challenges in cloud-IoT systems.

As in Fig. 5, based on a synthesis of 21 selected articles, security and privacy were the most dominant challenges, reported in 16 articles (76%). These challenges include data leaks, cyberattacks, identity verification, access controls, and the protection of sensitive information. The dominance of these challenges shows that the integration of IoT devices with cloud environments increases the need to protect data collected,

transmitted, and stored through interconnected infrastructure. Next, resource management and scalability were identified in 14 articles (67%), involving processing, storage, and energy constraints, as well as increased data volume and workload. This challenge arises because Cloud-Based IoT systems need to support the increase in devices and processing demands without compromising resource utilization and operational efficiency. Communication and processing performance were reported in 12 articles (57%), specifically related to latency, data transmission delays, response times, bandwidth usage, and real-time application requirements. These findings show that the efficiency of data transfer and processing is an important aspect to ensure that the system can meet the set service requirements.

In addition, integration and interoperability were reported in 11 articles (52%). These challenges stem from the heterogeneity of devices, communication protocols, data formats, and platforms used in the IoT–Cloud ecosystem. Such diversity can make it difficult for data exchange and integration between system components, thus demonstrating the need for appropriate communication mechanisms and integration approaches. Reliability challenges and system failures were identified in 5 articles (24%), involving node failure, single point of failure risk, connection stability, and system recovery. Although the percentage is lower, this challenge remains significant because interference with components or connections can affect the continuity of system operation. Meanwhile, the categories of rules and standards were reported in 6 articles (29%), covering the lack of common standards, uniform protocols, and compliance requirements. This issue is related to the difficulty of coordinating implementation and ensuring compatibility between different technologies. Legislation is recorded in 4 articles (19%). Based on the synthesis table, this category includes issues of lack of concrete metrics, tool support, Service Level Agreement (SLA) management, and service quality assessment. Therefore, this category needs to be interpreted based on the scope of coding used in the study, as its content also includes aspects of service management and measurement, not just legal obligations.

These findings were obtained through a systematic synthesis process of 21 selected articles, which involved identifying challenges in each article, comparing findings between studies, combining challenges with similar meanings, and grouping them into seven main categories. The process also involves repeated review to assess the suitability of the challenges with the set categories and reduce overlap between themes. The number of articles per category is then used to determine the percentage frequency, taking into account that an article can contribute to more than one category. This approach allows findings from various studies to be compiled in a more organized manner and provides a comprehensive picture of the challenges reported in Cloud-Based IoT systems.

Overall, this synthesis shows that Cloud-Based IoT challenges involve the relationship between security, resource management, performance, integration, reliability, and service management. These findings provide the basis for further analysis to map the challenges to nine characteristics of non-functional requirements (NFRs).

B. RQ2: What Are the Main Characteristics of Non-Functional Requirements (NFRs) Identified in Cloud-Based IoT Systems?

RQ1 uncovers the challenges that exist in cloud-IoT systems reported in the literature review, specifically those with implications for the development of non-functional requirements (NFRs). RQ2 extends the study by identifying the best NFR characteristics that address those challenges. In this context, the NFR list must adapt to any possible changes in operations or governance, such as big data, network environments, or other requirements.

The recent insights highlight that NFR serves not only as a quality attribute but also as a critical element that determines the effectiveness of system operations. This implies that systems must be able to handle large-scale data efficiently, securely, and stably in a dynamic environment. NFR is a quality characteristic. However, NFR also includes characteristics that determine how a system operates in terms of performance, security, and scalability.

A systematic analysis was carried out on the 21 studies selected for this review to identify the NFR characteristics reported in cloud-based IoT systems. Relevant information was examined and compared across the studies to identify common characteristics and organise them into meaningful categories that reflect the research context. Existing software quality models and NFR frameworks were also consulted to support the interpretation and classification of these characteristics. However, the classification was guided primarily by the findings reported in the selected studies, rather than by the characteristics defined in existing models alone. The findings were then synthesised to establish the main NFR characteristics identified in the literature and address RQ2.

This study uses a combined approach in the development of the NFR model for Cloud-Based IoT systems in Smart Governance. The SLR findings prove that there are challenges and some important NFR features, while ISO/IEC 25010:2023 is used as the main reference for ICT product quality structure [45]. In addition, classical quality models are used as a source of comparison of concepts such as McCall's [46], Boehm [47], FURPS [48], and Dromey [49], while the NFR Framework supports the analysis of the relationship between quality requirements [50]. Next, international digital government guidance and related policy documents are used to assess the suitability of NFR features in the context of Smart Governance such as Guidelines for the State's IT project model Vejledning til statens it-projektmodel from Denmark [51], Estonia ICT Development Guidelines Digital Public Administration Factsheet from Estonia [52], Internet of Things Cyber Security, Guidelines Internet of Things (IoT) Cyber Security Guide from Singapore [53], [54], eGovFrame Hands-on Guide for Developing Applications with the eGovernment Standard Framework from Korea [55] and Panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA) from Malaysia [56]. This combination allows the proposed model to be based on a literature review as a basis for quality and to consider the needs of the digital government context. Fig. 6 shows NFR characteristics that have been identified through the literature.

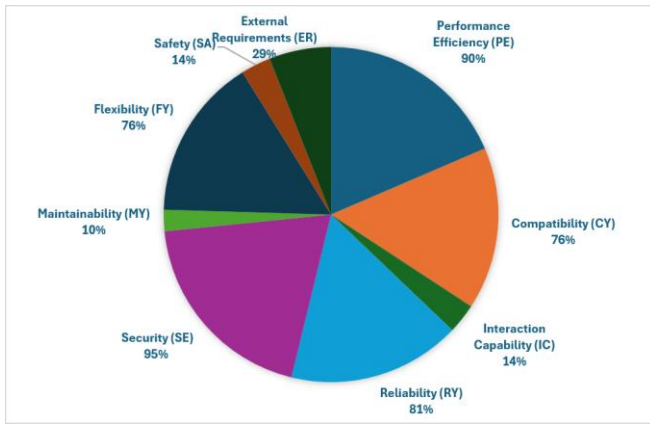


Fig. 6. Non-functional requirement characteristics cloud-based IoT.

Overall, the findings of Fig. 6 provide an overview of the distribution of the nine NFR features in the literature of cloud-based IoT systems. This analysis also helps to identify features that are under-appreciated and can be used as the basis for a more comprehensive study of cloud-based IoT systems in the context of Smart Governance.

Based on an analysis of 21 selected articles, Security (SE) was the most dominant NFR feature, with a percentage of 95%, followed by Performance Efficiency (PE) at 90% and Reliability (RY) at 81%. These findings show that security, performance efficiency, and reliability are the quality aspects that need the most attention in the Cloud-Based IoT literature. Next, Compatibility (CY) and Flexibility (FY) recorded 76% respectively, demonstrating the importance of compatibility between system components as well as the ability of the system to adapt to changing needs and workloads. External Requirements (ER) recorded 29%, while Interaction Capability (IC) and Safety (SA) were 14% each. In addition, Maintainability (MY) recorded the lowest percentage, at 10%.

Overall, these findings suggest that the literature focuses more on safety, performance, and reliability, while interaction capabilities, physical safety, and maintainability are underreported. This pattern identifies aspects that require further attention in NFR research of Cloud-Based IoT systems, without meaning that underreported features are not important.

Table II summarizes the SLR, revealing NFR characteristics, such as performance efficiency (PE), compatibility (CY), reliability (RY), security (SE), maintainability (MY), flexibility (FY), safety (SA), and external requirement (ER).

Table III shows the summary of NFR characteristics discovered from recent research and relevant studies focused on characteristics related to performance efficiency, security, and reliability, while aspects of interaction capability, compatibility, maintainability, flexibility, external requirement, and safety remain underexplored. This distribution is more specific to article matches. In addition, this article clearly mentions some of the quality features but doesn't necessarily elaborate on each feature in depth. Table III uses the rule that a mark “/” is given when there is relevant evidence from the literature.

TABLE III. NFR MAIN CHARACTERISTICS

Author	PE	CY	IC	RY	SE	MY	FY	SA	ER
[15]					/				
[57]	/	/		/	/	/	/		
[58]		/	/	/	/	/	/	/	
[59]	/				/				
[60]	/	/		/	/		/		
[9]	/	/		/	/		/		
[61]	/	/		/	/		/		/
[62]	/			/	/				/
[63]	/	/		/	/		/		/
[64]	/			/	/				
[13]	/	/		/	/		/		
[65]	/	/	/	/	/		/		/
[66]	/	/		/	/		/		
[27]	/	/		/	/		/		
[67]	/	/		/	/		/		/
[68]	/				/				
[69]	/	/		/	/		/		
[70]	/	/		/	/		/		
[71]	/	/	/	/	/		/	/	/
[72]	/	/		/	/		/	/	
[73]	/	/					/		

C. RQ3: What Are the Publication Trends in Cloud-Based IoT Studies Over the Years?

The analysis of 21 selected studies shows the publishing trends in this research field. This trend aligns with technological changes, indicating that this topic remains relevant for exploration in future modern technology. Fig. 7 shows the trend by year of publication.

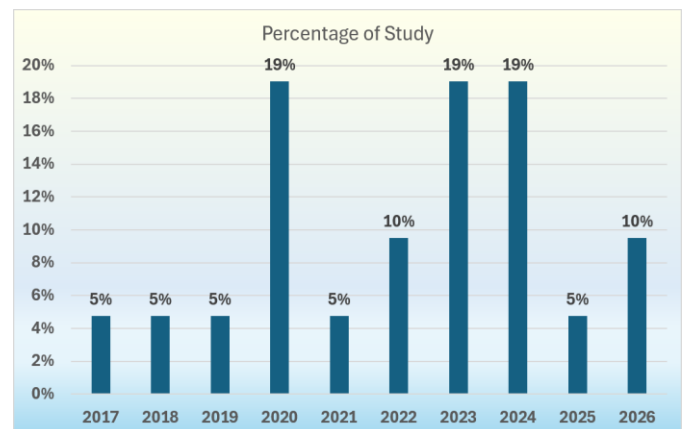


Fig. 7. Publication trends.

The analysis shows that starting from 2017, the trend in NFR-related studies on cloud-based IoT systems has grown inconsistently. The publication rate was low in the early stages, at only 5% per year between 2017 and 2019. However, the rate increased significantly to 19% starting in 2020. This indicates growing awareness among researchers of the importance of accurately collecting NFRs to address issues of performance, security, and reliability in cloud-based IoT systems. The following year, publications again declined to 5% in 2021 before rising to 10% in 2022. The highest number of publications in 2023 and 2024, at 19% each year, shows that NFR-related studies are gaining more attention in line with the development of IoT technologies, cloud computing, edge computing, and increasing data security requirements. However, the slight decrease to 5% in 2025 and a modest increase to 10% in mid-2026 are still developing and have not reached end of year which is expected to be more stable level of maturity.

Overall, these findings show that while NFR is important in developing cloud-based IoT systems, the number of studies is still limited. The trend of publications shows that research in this field is still developing, so there is an opportunity to explore more widely to strengthen understanding of the issues being studied.

V. CONCLUSION AND FUTURE STUDIES

The study identifies the main characteristics of NFR for cloud-based IoT systems using an SLR approach. The main characteristics include performance efficiency, compatibility, interaction capability, reliability, security, maintainability, flexibility, safety, and external requirements prioritized among NFRs for cloud-based IoT. These findings further strengthen the existing basic theories obtained from previous studies and make the development of this NFRs model more effective. Further studies are proposed to confirm this NFRs model through empirical studies such as expert interviews or industry case studies, as jointly planned.

The findings highlight the need for further research to establish a comprehensive approach to NFRs in cloud-based IoT systems. Although previous studies have identified a range of NFR characteristics, these characteristics are often considered separately, making it difficult to understand how they collectively address the quality needs of cloud-based IoT systems. Future research could therefore focus on developing a comprehensive NFR model, identifying its applicability through empirical studies, and performing a comprehensive experiment with different use-case scenarios in real-world cloud-based IoT system development. This would help determine whether the identified NFR characteristics are relevant and practical when applied to actual system development contexts, while also providing insights for further refinement of the proposed model.

VI. LIMITATIONS

The study had some limitations, starting with findings based on 21 selected articles from five databases and depending on the search strategy and selection criteria used. Next, the articles analysed included a wide range of studies, including literature reviews and mapping studies. Therefore, the challenges identified reflect issues reported in the Cloud-Based IoT literature and have not necessarily been empirically tested in real

systems. In addition, the process of grouping challenges into seven categories and mapping them to nine NFR characteristics involves the analytical considerations of researchers.

Despite these limitations, this study provides a structured synthesis of the challenges of Cloud-Based IoT and NFR features reported in the literature. Analysis of publication trends provides a descriptive picture of the distribution of selected studies but does not necessarily reflect the overall maturity of this field. The findings of the study can be used as a basis for identifying research gaps, conducting further empirical studies, and supporting the development and validation of the NFR model in the future.

REFERENCES

- [1] M. Almutairi and F. T. Sheldon, "IoT-Cloud Integration Security: A Survey of Challenges, Solutions, and Directions," Apr. 01, 2025, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/electronics14071394.
- [2] K. S. Lim, S. Y. Ooi, M. S. Sayeed, Y. J. Chew, and N. M. Ahmad, "Securing the Internet of Things: Systematic Insights into Architectures, Threats, and Defenses," Oct. 01, 2025, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/electronics14203972.
- [3] M. Papatismouli, L. Lazaridis, D. Ziouzos, M. Dasygenis, and G. Fragulis, "Internet of Things (IoT) awareness in Greece," SHS Web of Conferences, vol. 139, p. 03013, 2022, doi: 10.1051/shsconf/202213903013.
- [4] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "IoT Threat Detection Advances, Challenges and Future Directions," in Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT 2020, Institute of Electrical and Electronics Engineers Inc., Apr. 2020, pp. 22–29. doi: 10.1109/ETSecIoT50046.2020.00009.
- [5] J. O. V. Paiva, R. M. Carvalho, and R. M. C. Andrade, "Towards a Process for NFRs Evaluation in IoT Applications," 2022.
- [6] Z. Bo, M. K. Hasan, E. A. Sundararajan, T. R. Gadekallu, and S. Islam, "An Adaptive Simulated Annealing Algorithm for Optimizing Task Scheduling in Internet of Things," in Proceedings of 2025 6th International Conference on Computer Information and Big Data Applications, CIBDA 2025, Association for Computing Machinery, Inc, Aug. 2025, pp. 1494–1501. doi: 10.1145/3746709.3746967.
- [7] A. Waqar, M. B. Khan, N. Shafiq, K. Skrzypkowski, K. Zagórski, and A. Zagórska, "Assessment of Challenges to the Adoption of IOT for the Safety Management of Small Construction Projects in Malaysia: Structural Equation Modeling Approach," Applied Sciences (Switzerland), vol. 13, no. 5, 2023, doi: 10.3390/app13053340.
- [8] U. Wahida et al., "Internet of Things: An Implementation and Its Challenges in Malaysia," vol. 8, no. 6, 2018.
- [9] M. Saeed Alshahrani et al., "Integrating Cloud Computing and Internet of Things: A Systematic Review of Literature," IJCSNS International Journal of Computer Science and Network Security, vol. 25, no. 5, 2025, doi: 10.22937/IJCSNS.2025.25.5.23.
- [10] T. A. N. Abdali, R. Hassan, A. H. M. Aman, and Q. N. Nguyen, "Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues," IEEE Access, vol. 9, pp. 75961–75980, 2021, doi: 10.1109/ACCESS.2021.3081770.
- [11] N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," Jan. 01, 2025, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/s25010079.
- [12] T. R. Merlo, F. Fard, and S. Hawamdeh, "Cloud Computing's Impact on the Digital Transformation of the Enterprise: A Mixed-Methods Approach," Sustainability (Switzerland), vol. 17, no. 13, Jul. 2025, doi: 10.3390/su17135755.
- [13] F. Karim, "Integration of IoT and Cloud Computing: A Systematic Review," 2024.
- [14] F. Mohd Ali, M. Mat Daud, and R. Latip, "Sustainable Data Placement Strategy for Energy-Efficient Cloud Storage and Enhanced Performance,"

- in E3S Web of Conferences, EDP Sciences, Nov. 2025. doi: 10.1051/e3sconf/202565903004.
- [15] N. Kashyap, A. Rana, V. Kansal, and H. Walia, "Improve Cloud Based IoT Architecture Layer Security - A Literature Review," in Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCIS 2021, Institute of Electrical and Electronics Engineers Inc., Feb. 2021, pp. 772–777. doi: 10.1109/ICCIS51004.2021.9397146.
- [16] G. Gondhalekar, D. Tewari, B. P. I. Bhardwaj, S. Ponnusamy, and A. S., "Internet of Things Integration in Smart Cities Enhancing Urban Living through Connected Technologies," ITM Web of Conferences, vol. 76, p. 03001, 2025, doi: 10.1051/itmconf/20257603001.
- [17] D. Verma, "Integrated System: IoT and Cloud Computing," 2022. [Online]. Available: <https://www.researchgate.net/publication/372187556>
- [18] F. Noviyanto, R. Razali, and M. Z. A. Nazri, "Understanding requirements dependency in requirements prioritization: a systematic literature review," International Journal of Advances in Intelligent Informatics, vol. 9, no. 2, pp. 249–272, Jul. 2023, doi: 10.26555/ijain.v9i2.1082.
- [19] Z. Daud, S. Ya, N. Azaliah Abu Bakar, S. Sumarni Hussein, T. Malaysia, and T. Mara Shah Alam, "A Review for Analytics Requirements Processes: From Malaysia Public Sector Perspectives Article history," 2022.
- [20] A. Fariha, S. Alwidian, and A. Azim, "A Systematic Literature Review on Requirements Engineering and Maintenance for Embedded Software," IEEE Access, vol. 12, pp. 114263–114279, 2024, doi: 10.1109/ACCESS.2024.3443271.
- [21] M. R. H. Roslan, K. Ahmad, and M. M. Ayyash, "Factors Influencing Information Systems Quality From The System Developers Perspective," Asia-Pacific Journal of Information Technology and Multimedia, vol. 09, no. 01, pp. 82–93, Jun. 2020, doi: 10.17576/apjitm-2020-0901-07.
- [22] N. Alhirabi, O. Rana, and C. Perera, "Security and Privacy Requirements for the Internet of Things," ACM Transactions on Internet of Things, vol. 2, no. 1, pp. 1–37, Feb. 2021, doi: 10.1145/3437537.
- [23] J. Yahaya, A. Deraman, and Z. H. Abdullah, "Software Product Quality: Trends and Beyond," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 64, no. 3, pp. 8–20, Mar. 2025, doi: 10.37934/araset.64.3.820.
- [24] D. Gobov and O. Zuieva, "Software Quality Attributes in Requirements Engineering," International Journal of Information Technology and Computer Science, vol. 17, no. 4, pp. 38–48, Aug. 2025, doi: 10.5815/ijitcs.2025.04.04.
- [25] N. H. Ramli, N. Atiqah, S. Abdullah, N. Ida, and A. Rusli, "A Systematic Review of Functional Requirements, Modelling Practices, and Validation Strategies in IoT Application Development," 2025. [Online]. Available: www.ijacsa.thesai.org
- [26] B. Mahanta et al., "Privacy-Preserving Strategies for Secure Cloud of Things: A Review of Current Approaches," Institute of Electrical and Electronics Engineers (IEEE), Nov. 2025, pp. 1–6. doi: 10.1109/ccpis65231.2025.11233919.
- [27] S. Medjah and C. Chassot, "On the enhancement of non-functional requirements for cloud-assisted middleware-based IoT and other applications," 2020.
- [28] M. Nouman, M. Azam, A. M. Saleh, A. Alsaeedi, and H. Y. Abuaddous, "A systematic review of non-functional requirements mapping into architectural styles," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 2, pp. 1226–1236, Apr. 2023, doi: 10.11591/eei.v12i2.4081.
- [29] E. K. Budiardjo and W. C. Wibowo, "Non-functional Requirements (NFR) Identification Method using FR Characters based on ISO/IEC 25023," 2021. [Online]. Available: www.ijacsa.thesai.org
- [30] A. Bhar et al., "A Domain-Specific Framework for Priority-Based Modeling and Optimization of Non-Functional Requirements Beyond Binary Constraints," IEEE Access, 2026, doi: 10.1109/ACCESS.2026.3666268.
- [31] A. Bhar, S. Sengupta, and S. Choudhury, "Aspect-Oriented Approach of Non-Functional Requirements for Embedded System-Based IoT Applications," IEEE Access, vol. 13, pp. 129451–129460, 2025, doi: 10.1109/ACCESS.2025.3585417.
- [32] A. Shabbir, A. Deraman, M. N. Bin Hassan, K. U. Sarker, and S. Kamal, "Prioritizing Non-Functional Requirements and Influencing Factors for API Quality Framework: An Industry Approach," International Journal of Advanced Computer Science and Applications, vol. 16, no. 9, 2025, doi: 10.14569/ijacsa.2025.0160934.
- [33] E. Rashid and N. E. Mastorakis, "A Novel Complexity Scoring Model for Non-Functional Requirements in Request for Proposal in Housing Industry Using FURPS Quality and Moscow Priority Model," International Journal for Housing Science and Its Applications, vol. 45, no. 4, pp. 30–40, Dec. 2024, doi: 10.70517/ijhsa4543.
- [34] S. S. Paradkar, "A Framework for Modeling Non Functional Requirements for Business Critical Systems," International Journal of Innovative Research in Computer Science & Technology, vol. 9, no. 1, pp. 15–19, Jan. 2021, doi: 10.21276/ijircst.2021.9.1.3.
- [35] A. Muhammad, A. Siddique, M. Mubasher, A. Aldweesh, and Q. N. Naveed, "Prioritizing Non-Functional Requirements in Agile Process Using Multi Criteria Decision Making Analysis," IEEE Access, vol. 11, pp. 24631–24654, 2023, doi: 10.1109/ACCESS.2023.3253771.
- [36] J. Cai and Y. He, "Automatic Classification of Non-Functional Requirements Based on Deep Pre-Trained Models," in 2026 5th International Symposium on Computer Applications and Information Technology (ISCAIT), IEEE, Jan. 2026, pp. 976–979. doi: 10.1109/ISCAIT69154.2026.11477396.
- [37] N. Fadilah Najwa, M. A. Furqon, and F. Mahananto, "Literature Review on Extended Use case in Modeling Non-functional Requirement," International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT, vol. 3, no. 3, pp. 1832–1844, 2018.
- [38] M. R. Tabassum, "Addressing non-functional requirements of adaptive IoT Systems: A model-driven approach," in Proceedings - ACM/IEEE 25th International Conference on Model Driven Engineering Languages and Systems, MODELS 2022: Companion Proceedings, Association for Computing Machinery, Inc, Oct. 2022, pp. 195–200. doi: 10.1145/3550356.3558514.
- [39] J. T. Almonte, S. A. Boominathan, and N. Nascimento, "Automated Non-Functional Requirements Generation in Software Engineering with Large Language Models: A Comparative Study," Mar. 2025, [Online]. Available: <http://arxiv.org/abs/2503.15248>
- [40] H. Aljohani, H. W. Ghandorh, and W. M. S. Yafooz, "Functional and Non-Functional Requirements Classification and Artificial Intelligence: A Survey," in 2026 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA), IEEE, Feb. 2026, pp. 1–9. doi: 10.1109/ACDSA67686.2026.11468107.
- [41] H. Al Akbar, M. R. Faturrahman, and S. Sidharta, "Guidance in Designing A Smart Campus: A Systematic Literature Review," in Procedia Computer Science, Elsevier B.V., 2023, pp. 83–91. doi: 10.1016/j.procs.2023.10.505.
- [42] R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic Literature Review on Security Risks and its Practices in Secure Software Development," 2022, Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ACCESS.2022.3140181.
- [43] Kitchenham & Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," 2007.
- [44] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," J. Clin. Epidemiol., vol. 134, pp. 178–189, Jun. 2021, doi: 10.1016/j.jclinepi.2021.03.001.
- [45] P. Ariningsih and A. H. Muhammad, "Quality Evaluation of Ticketing Management System Using ISO/IEC25010:2023 Standards and AHP Method," Journal : Information Technology Journal, vol. 6, no. 2, 2024.
- [46] A. Jameel Al-nawaiseh, F. Bani Ahmad, and S. Jamil Al-nawaiseh, "A Critical Review of Software Quality Models in Academic Information System," 2024. [Online]. Available: www.jatit.org
- [47] A. A. Magableh, A. A. Saifan, A. Rawashdeh, and H. B. Ata, "Towards Improving Aspect-Oriented Software Reusability Estimation," Jul. 07, 2023. doi: 10.21203/rs.3.rs-3124387/v1.
- [48] G. L. Saini and D. Panwar, "Comparative Study of Open Source Software Quality Models," 2020. [Online]. Available: <https://n2t.net/ark:/47543/JISCOM2020.v1i1.a7>

- [49] N. Bitew and J. Singh, "A Study on Software Quality Factors and Metrics to Enhance Software Quality Assurance," *International Journal of Productivity and Quality Management*, vol. 1, no. 1, p. 1, 2019, doi: 10.1504/ijpqm.2019.10025496.
- [50] L. Chung, J. C. Sampaio, and P. Leite, "On Non-Functional Requirements in Software Engineering," 2009. [Online]. Available: www.utdallas.edu/~chung/, www.inf.puc-rio.br/~julio
- [51] Økonomistyrrelsen, "Vejledning til statens it-projektmodel," 2024.
- [52] Digital Europe Programme, "Digital Public Administration Factsheet," 2024.
- [53] IMDA, "Guidelines Internet of Things (IoT) Cyber Security Guide," 2022. [Online]. Available: <http://www.imda.gov.sg>
- [54] IMDA, "Internet of Things (IoT) Cyber Security Guide," 2025. [Online]. Available: <http://www.imda.gov.sg>
- [55] eGovFrame, "Hands-on Guide for Developing Applications with the eGovernment Standard Framework," 2025.
- [56] Jabatan Digital Negara, "BAB3 ANALISIS DATA (KRISA)," 2026.
- [57] M. N. Jahantigh, A. M. Rahmani, N. J. Navimirour, and A. Rezaee, "Integration of Internet of Things and cloud computing: A systematic survey," Jan. 17, 2020, *Institution of Engineering and Technology*. doi: 10.1049/iet-com.2019.0537.
- [58] H. P. Breivold, "Internet-of-Things and Cloud Computing for Smart Industry: A Systematic Mapping Study," in *Proceedings - 2017 5th International Conference on Enterprise Systems: Industrial Digitalization by Enterprise Systems*, ES 2017, Institute of Electrical and Electronics Engineers Inc., Nov. 2017, pp. 299–304. doi: 10.1109/ES.2017.56.
- [59] G. Luo, Z. Chen, and B. O. Mohammed, "A systematic literature review of intrusion detection systems in the cloud-based IoT environments," *Concurr. Comput.*, vol. 34, no. 10, May 2022, doi: 10.1002/cpe.6822.
- [60] S. Shukla, M. F. Hassan, D. C. Tran, R. Akbar, I. V. Paputungan, and M. K. Khan, "Improving latency in Internet-of-Things and cloud computing for real-time data transmission: a systematic literature review (SLR)," *Cluster Comput.*, vol. 26, no. 5, pp. 2657–2680, Oct. 2023, doi: 10.1007/s10586-021-03279-3.
- [61] H. Kuchuk and E. Malokhvii, "Integration of IoT With Cloud, Fog, And Edge Computing: A Review," *Advanced Information Systems*, vol. 8, no. 2, pp. 65–78, Jun. 2024, doi: 10.20998/2522-9052.2024.2.08.
- [62] P. Kaur, R. Handa, and M. Kanaujia, "Securing Internet of Things Devices in the Cloud - A Literature Review," in *Proceedings - 2024 2nd International Conference on Advanced Computing and Communication Technologies*, ICACCTech 2024, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 631–636. doi: 10.1109/ICACCTech65084.2024.00106.
- [63] C. Surianarayanan and P. R. Chelliah, "Integration of the Internet of Things and Cloud: Security Challenges and Solutions - A Review," 2023, IGI Global. doi: 10.4018/IJCAC.325624.
- [64] S. Mubeen, S. A. Asadollah, A. V. Papadopoulos, M. Ashjaei, H. Pei-Breivold, and M. Behnam, "Management of Service Level Agreements for Cloud Services in IoT: A Systematic Mapping Study," *IEEE Access*, vol. 6, pp. 30184–30207, 2018, doi: 10.1109/ACCESS.2017.2744677.
- [65] L. Albshaier, A. Budokhi, and A. Aljughaiman, "A Review of Security Issues When Integrating IoT With Cloud Computing and Blockchain," *IEEE Access*, vol. 12, pp. 109560–109595, 2024, doi: 10.1109/ACCESS.2024.3435845.
- [66] S. Girs, S. Sentilles, S. A. Asadollah, M. Ashjaei, and S. Mubeen, "A Systematic Literature Study on Definition and Modeling of Service-Level Agreements for Cloud Services in IoT," 2020, Institute of Electrical and Electronics Engineers Inc. doi: 10.1109/ACCESS.2020.3011483.
- [67] S. Chahar, K. S. Kaswan, A. Aggarwal, and J. S. Dhatteval, "New Era of IoT with Cloud Computing: A review of Technology, Issues and Challenges," in *2024 2nd International Conference on Advancements and Key Challenges in Green Energy and Computing*, AKGEC 2024, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/AKGEC62572.2024.10868472.
- [68] B. Alobaywi, M. G. Almutairi, and F. T. Sheldon, "Performance Trade-Offs in Multi-Tenant IoT-Cloud Security: A Systematic Review of Emerging Technologies," Mar. 01, 2026, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/iot7010021.
- [69] S. Dutta and R. Sharma, "A Review on the Current Techniques of Sustainable Cloud Computing Framework for the IOT-Enabled Smart Cities," 2026.
- [70] P. Goudarzi, A. M. Rahmani, and M. Mosleh, "Resource discovery approaches in cloudIoT: a systematic review," *Journal of Supercomputing*, vol. 78, no. 15, pp. 17202–17230, Oct. 2022, doi: 10.1007/s11227-022-04541-0.
- [71] C. Butpheng, K. H. Yeh, and H. Xiong, "Security and privacy in IoT-cloud-based e-health systems-A comprehensive review," *Symmetry (Basel)*, vol. 12, no. 7, Jul. 2020, doi: 10.3390/sym12071191.
- [72] L. Gholamhosseini, A. Behmanesh, S. Nasiri, S. J. Ehsanzadeh, and F. Sadoughi, "Cloud-based Internet of Things in healthcare applications: A systematic literature review," 2023, *Iranian Medical Informatics Association (IrMIA)*. doi: 10.30699/fhi.v12i0.451.
- [73] E. L. C. Macedo et al., "On the security aspects of Internet of Things: A systematic literature review," Oct. 01, 2019, *Korean Institute of Communication Sciences*. doi: 10.1109/JCN.2019.000048