Albahit Journal of Applied Sciences
"open-access, peer-reviewed biannual journal"
eISSN: 2708-8936, pISSN: 2708-244X
Volume 5, Issue 2, 2026
Page No: 185-209
***Website**: https://albahitjas.com.ly/index.php/albahit/en/index*

Integration of the Internet of Things with Cloud Computing: Security Challenges, Performance Issues, and Future Directions

Hend ALmezoghy [1*] , Mabruka Ibrahim [2]
[1,2] Department of Information Technology, Al-Zaytouna University, Tarhuna, Libya
[*]*Corresponding author:* hmezoghi@gmail.com

Received: 15-03-2026	**Accepted:** 02-05-2026	**Published:** 16-05-2026

Abstract:
The current increase in Internet of Things (IoT) applications requires transmitting, storing, and processing tremendous amounts of data. To fulfill these specific application needs, many IoT applications require the use of cloud computing. Nevertheless, integrating the IoT with the cloud also has problems with network latency, throughput, energy consumption, reliability, and so on. Thus, a new computing model is required to support the future use of IoT. This paper examines the performance of IoT in cloud computing, its issues, potential solutions, and prospects. The primary purpose of the investigation of the collaboration of IoT and cloud computing technologies and the optimization of information management and decision-making is a combination of the two that can introduce new security concerns.
The method focuses on practical applications and security vulnerabilities by conducting an extensive literature review and case studies in various industries, such as smart infrastructure and healthcare. Findings indicate that cloud computing and IoT improve scalability, cost efficiency, and real-time data accessibility. The aspects of this integration include critical security concerns like real-time access to data, AI attacks by adversaries, and limitations that are imposed by limited IoT devices. To maintain system resilience, the research of the future should be focused on enhancing privacy protection and fighting the emergent threats.

Keywords: Security, IoT Security, Network Latency, Data Management, Artificial Intelligence.

دمج إنترنت الأشياء مع الحوسبة السحابية: تحديات الأمن، ومشكلات الأداء، والتوجهات المستقبلية

هند المزغي[1*]، مبروكة إبراهيم[2]
[2،1] قسم تقنية المعلومات، جامعة الزيتونة، ترهونة، ليبيا.

الملخص
الانتشار الواسع للحوسبة السحابية (Cloud Computing) قد سرع في تطوير ونشر تطبيقات إنترنت الأشياء (IoT) وتكاملها إن انترنت الأشياء والحوسبة السحابية تقنيتان مختلفتان تماماً، ولكنهما تعتبران جزءاً أساسياً من مستقبل الإنترنت، يتطلب النمو الحالي في تطبيقات إنترنت الأشياء (IoT) نقل وتخزين ومعالجة كميات هائلة من البيانات. ولتلبية هذه الاحتياجات يتطلب استخدام الحوسبة السحابية. ومع ذلك، فإن دمج إنترنت الأشياء مع السحابة ينطوي أيضًا على مشاكل تتعلق بزمن وصول الشبكة، والإنتاجية، واستهلاك الطاقة، والموثوقية، وغيرها. لذا، يلزم نموذج حوسبة جديد لدعم الاستخدام المستقبلي لإنترنت الأشياء. تتناول هذه الورقة البحثية أداء إنترنت الأشياء في الحوسبة السحابية، ومشاكله، والحلول المحتملة، وآفاقه. الهدف الرئيسي من دراسة تكامل تقنيات إنترنت الأشياء والحوسبة السحابية، وتحسين إدارة المعلومات واتخاذ القرارات، تركز هذه الطريقة على التطبيقات العملية وثغرات الأمن من خلال إجراء مراجعة شاملة للأدبيات ودراسات حالة في قطاعات مختلفة، مثل البنية التحتية الذكية والرعاية الصحية. تشير النتائج إلى أن الحوسبة السحابية وإنترنت الأشياء

يُحسّنان قابلية التوسع، وكفاءة التكلفة، وإمكانية الوصول إلى البيانات في الوقت الفعلي. تشمل جوانب هذا التكامل مخاوف أمنية حرجة، مثل الوصول الفوري إلى البيانات، وهجمات الذكاء الاصطناعي التي يشنها الخصوم، والقيود التي تفرضها أجهزة إنترنت الأشياء المحدودة. وللحفاظ على مرونة النظام، ينبغي أن تركز أبحاث المستقبل على تعزيز حماية الخصوصية ومكافحة التهديدات الناشئة.

الكلمات المفتاحية: إنترنت الأشياء، الحوسبة السحابية، تكامل التقنيات، أمن المعلومات، أمن إنترنت الأشياء، زمن الوصول إلى الشبكة.

1. Introduction

The Internet of Things (IoT) is a collection of various tangible items or entities. To provide a better facility, this setup uses sensors, microelectronics, and software to send and receive data with a range of other relevant devices (Walia and Garg, 2022). With the aid of a technical stack that enables smooth communication between real and virtual devices, the Internet of Things (IoT) is an internetworking paradigm that makes it possible to construct intelligent services. Over the past several years, IoT-enabling technologies have become more proficient. As a result, new large-scale applications are now possible. However, due to resource constraints, IoT devices usually have restricted computational, communication, and other capabilities (Čolaković, 2023).

According to Aslanpour et al. (2020), cloud computing is a useful instrument that offers a variety of services, including infrastructure, software, and platforms. -Offloading services on IoT devices by various computer systems can get around the issue (Čolaković, 2023). In the context of IoT system modeling, the idea of compute offloading is regarded as a decision-making issue, with the goal being to select the best option given the resources at hand. The offloading idea is used to improve system performance by moving resource-intensive tasks to platforms or other infrastructures with more resources (Abdulazeez and Askar, 2023). This method allows devices with limited resources to save resources and increase their working life. Because there is no need to put undue burden on individual devices as IoT systems develop, offloading allows for more efficient use of computer resources to keep up with the growing number of devices linked to computer resources. By enabling the IoT system to accomplish tasks with more potent computing resources, offloading also improves performance by lowering energy consumption and reaction time. Optimizing resource efficiency and meeting system performance requirements is made achievable by including the notion of computational offloading into the modeling of IoT systems. IoT system modeling will assist in simulating several allocation strategies and choosing the one that will minimize costs or maximize system performance (Čolaković, 2023).

However, latency, bandwidth needs, security, and dependability are additional issues that arise when the IoT and cloud are integrated. We looked into fog computing, a novel distributed computing platform, to ascertain the requirements of government IoT applications that are latency-sensitive. The majority of Internet of Things devices have the least amount of security. Since they are still in use, several of these devices are not adequately updated. Due to their antiquated hardware and software, the devices will be vulnerable to potential assaults (Kutzias et al., 2019). With the advent of PCs, first on the internet and later in cloud computing, the globe is seeing significant technical advancements or changes (Fotouhi et al., 2017). Since networking equipment and other organizations are still in their infancy, the product's approach does not address the fundamental problem of security. IoT devices typically come with an operating system and software that are out of date and difficult to fix.

1.1 Research Problem

The Internet of Things (IoT) and cloud computing technologies are rapidly progressing, but making them work together efficiently is a challenge. Cloud computing offers scalable storage, processing power and flexible management of resources for IoT applications, but this comes

with a number of related securities, privacy, latency, interoperability, energy use, reliability, and real-time responsiveness challenges. Previous research primarily focuses on one aspect of these problems, such as security mechanisms or system performance, and few works address the basic problem of meeting all of these requirements within a single IoT–cloud system. Therefore, there is a need for a thorough review that encompasses the state of the art on security, performance, scalability, and privacy, and the possibility to address them all simultaneously in the context of a reliable and sustainable IoT–cloud integration.

This study expands the scope of the research on IoT–cloud security, as it covers discussions on adversarial AI threats, lightweight cryptographic methods for restricted IoT devices, API security best practices, and a transition to post-quantum security in IoT-cloud systems. The paper provides a better map of the direction that future research should take and contributes to the existing body of knowledge.

The study looks at the problems, solutions, and potential developments of IoT collaboration in cloud computing. The collaboration between cloud computing and the Internet of Things will begin by outlining how these two technologies combine to make managing data across multiple devices easier. This partnership makes it easier to handle, store, and analyze data quickly, which makes it a vital tool for improving decision-making and producing precise projections. However, security concerns have been raised by the combination of these technologies. To determine the presence or absence of solutions to its challenges, this study reviews and examines the possibility of enhancing the security of cloud computing and the Internet of Things. Future directions should also be suggested by us. Finally, the study will ensure the security and security of cloud computing and the IoT in case they are integrated. The objectives of the study can be summarized as follows:

- To examine the ways in which cloud computing and IoT technologies might be integrated and cooperate.
- to emphasize the advantages of integrating cloud computing and IoT for cost savings, scalability, data processing, and prediction.
- To determine the expanding security concerns in cloud and Internet of Things networks.
- To assess the security solutions utilizing cloud computing and Internet of Things technologies.
- To investigate how IoT and cloud computing integration may affect privacy and security in the future.

1.3 Research Questions

To achieve the objectives of this review, the study seeks to answer the following research questions:

- RQ1: What are the primary technical challenges associated with integrating Internet of Things (IoT) systems with cloud computing environments?
- RQ2: How do performance-related factors—including latency, scalability, reliability, energy consumption, and real-time responsiveness—influence the effectiveness of IoT–cloud integration?
- RQ3: What are the major cybersecurity and privacy challenges affecting IoT–cloud environments, and what solutions have been proposed in recent research?
- RQ4: How do cloud computing, fog computing, and edge computing compare in supporting IoT applications with respect to performance, security, scalability, and deployment requirements?
- RQ5: What insights can be derived from representative smart infrastructure and smart healthcare case studies regarding the practical implementation of IoT–cloud systems?
- RQ6: What research gaps and emerging directions should be addressed to improve the performance, security, and sustainability of future IoT–cloud ecosystems?

1.4 Conceptual model

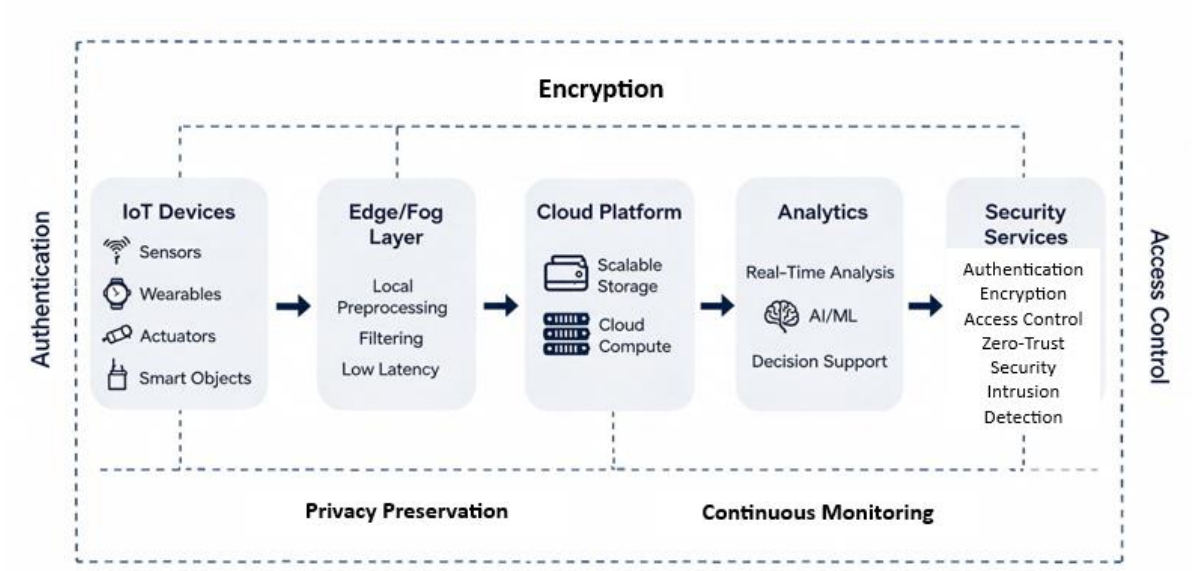

Figure 1 *Conceptual model of IoT devices, edge/fog computing, cloud platforms, analytics, and integrated security services.*

Figure 1, presents the conceptual architecture IoT–cloud integration used in this review is represented. The conceptual architecture IoT–cloud integration used in this review is presented in Figure 1. The framework represents the data moving from the IoT devices to the edge/fog layer for low latency processing, and then to the cloud for storage and computation. The data is then processed, analyzed with AI based analytics for intelligent decision making. All architectural layers include cross-layer security mechanisms in order to have secure, reliable and scalable IoT–cloud operation, such as authentication, encryption, access control, privacy preservation and continuous monitoring.

2. Related Work

2.1 Security and Privacy of IoT

The emergence of cloud computing and the Internet of Things has completely changed how we use technology and handle information. The network of physical things with sensors, software, and other technologies that allow them to interact and share data with other objects over the internet is known as the Internet of Things. This applies to household appliances and fitness trackers that use these smart gadgets, as well as to city infrastructure and industrial machinery. Many parts of our everyday lives and work activities may be monitored, controlled, and optimized with the help of the Internet of Things (Sutikno and Thalmann, 2022).

Since it offers a security framework for web-based applications, network security has become more important in recent years. In order to prevent contemporary assaults, protection becomes crucial. The two main characteristics of the current assaults are the uncertainty of secrecy and the mitigation of attacks. Information is encoded by cryptography and decoded by the key holder.

Cryptography provides a guarantee that the data being transferred has not been tampered with. A scientific task discard known as a cryptographic technique, or cryptogram, is used in the encryption and decryption process. A key is a string of letters, numbers, or special symbols that is used in the cryptography process to encrypt plaintext. The plaintext can be transformed into distinct encrypted contents and encrypted with different keys. The confidentiality of the key and the strength of the set of rules that comprise the encryption process define the encryption statistics (Walia and Garg, 2022).

The price tag and the use of well-known cryptographic algorithms (DES, 3DES, AES, RSA, and Blowfish) were the main topics of Patil et al. (2016). Out of all these procedures, Blowfish is known to have the greatest entropy number, making it the most effective method for thwarting a guessing assault. Additionally, Poonia et al. (2015) improved the Blowfish procedure and assessed it using different constraints. The authors looked into the importance of encryption in the Internet of Things as well as other IoT security techniques (Suresh et al., 2016; Suresh and Neema, 2016). Several comparisons reveal that Blowfish is an effective encryption technique. Bruschi et al. (2017) proposed an intercommunication layer that, depending on the operator's location, permits the physical isolation of assets but limits the mobility of facility instances. Common encryption techniques, including symmetric (DES, Blowfish, AES) and asymmetric (ECC, RSA), have been compared by Mota et al. (2017). When it comes to completion time, memory use, throughput, power consumption, security, and IoT interoperability, Blowfish is regarded as the finest. Stergiou et al. (2018) focused on the issue of both technologies' security while assessing the capabilities of cloud computing and the Internet of Things. The author combines the two aforementioned skills to examine the common topographies and illustrates the benefits of doing so. In their IoT security article, Nandy et al. (2019) focused on validation methods. The author brought forth realistic approaches and sincere attempts on the verification process of the IoT verification mechanism, implying that the existing security authentication protocols and evaluation frameworks of IoT validation are inadequate. In their overview of recent RPL research, Kamguee et al. (2018) pointed out some helpful recommendations for enhancing the system, especially in the areas of topology optimization, security, and mobility.

The four main Internet of Things modules are recognition, data handling, applications and facilities, varied access, and auxiliary modules, which include security and confidentiality, according to Malge and Singh (2019). In terms of IoT layers, the author offered a secure perspective. In order to concentrate on the issue of security and confidentiality, Adamou et al. (2024) talked about some of the likely issues and hazards that need to be addressed. In order to do this, the author looked at the architecture of the Internet of Things and its current uses. They also talked about the difficulties and concerns related to security and confidentiality. Kutzias et al. (2019) developed a generic integration design to complement their proposal of the many integration contests. The goal, the research done in this area, the variety of skills, and the future growth of the edge computing backdrop were all covered by Vijayalakshmi et al. (2019). In their study of cloud providers, Kaur et al. (2020) offered a pay-as-you-use prototype in which users only paid for the specific resources they used. In a similar vein, cloud computing capabilities are valuable to IoT enterprises since they lower the total cost of configuration of the business through cost-cutting of scale.

2.2 Cloud Computing

In turn, the so-called cloud computing technology enables users to access and control computer resources, including databases, servers, storage, and applications, via the internet. Instead of depending on local hardware and software, cloud computing may offer a scalable and adaptable environment where resources can be readily handled. Among its many advantages are cost savings, more adaptability, and the capacity to manage massive volumes of data (Almutairi and Sheldon, 2025).

As cloud services become more widely used, more orchestration issues are emerging. The demand for popular online apps, for instance, increases throughout working hours, varies significantly around lunchtime, and declines between night and morning, according to Al-Dhuraibi et al. (2018). When dynamic resource provisioning is unable to handle this unpredictability, users may have to wait a very long time for a response. Resource allocation, resource provisioning, task scheduling, load balancing, server consolidation, task placement,

Virtual Machine (VM) migration, service composition, data caching, service discovery, and so forth are a few examples of orchestration techniques.

According to Gonzalez et al. (2016), cloudlets are another subclass of edge computing that is helpful for mobile systems, while mists are another subclass of edge computing that is accessible through the Internet of Things. With reference to the current state of the art and its future, the author categorized the major research fields that center around edge computing in a thorough review of relevant themes. A well-written, methodical study on resource management in relation to cloud resource planning and cloud computing in general may be found in Singh et al. (2015). Wazir et al. (2016) offer a wide range of strategies anticipated in the realm of SLA in cloud computing to handle the issues surrounding SLA. With the aid of tables, the advantages and disadvantages of the current cloud service models—such as SaaS, PaaS, and IaaS—as well as the difficulties related to performance, client-level fulfillment, security, profit, and SLA defilement are examined, along with the SLA design in cloud computing. According to Padmaja et al. (2022), programming increases the load of cloud computing applications by taking on the job of promoting maximum profit.

2.3 Cloud Service Models and Security

In addition to virtual computers, storage, and networking, Infrastructure as a Service (IaaS) also makes computer resources accessible online as virtual resources. It is also utilized for data storage, networking, and computer resource scaling. IaaS offers customers utility services that virtualize computer resources like servers and storage. Online hardware and software technologies (such as databases, middleware, and development frameworks) that are often used to create applications are offered by Platform as a Service (PaaS). It is frequently used by developers to create, launch, and maintain applications without having to worry about the supporting infrastructure. Rather than requiring separate configuration, PaaS provides middleware and APIs inside the development environments, enabling the creation of unique applications. Additionally, Software as a Service (SaaS) offers software programs for a monthly subscription cost. Additionally, its software applications and user interfaces are completely functional. SaaS products. A web browser may be used to access SaaS products, such as email services, CRM software, and collaborative tools. Additionally, SaaS is utilized to access cloud apps or pay per usage (Gibson et al., 2012).

Even though cloud computing offers many advantages, there are serious security issues, such as insider threats, data leaks, compliance issues, and unauthorized access (Aijaz et al., 2024; Tiwari and Pangerkar, 2024). Making sure that data integrity, privacy, and secrecy are met is the answer to these issues (Aijaz et al., 2024). Access controls and authentication can be enhanced by identity and access management, or IAM (Aijaz et al., 2024; Mallisetty et al., 2023). Other problems include safeguarding the cloud orchestration platform, guaranteeing service availability, and addressing the security threat posed by cloud-native apps (Aijaz et al., 2024). Cyberattacks, misuse of cloud resources, and unsecured APIs are the most frequent dangers (Mallisetty et al., 2023). Strong access controls, encryption, API security measures, enhanced encryption, virtual firewalls, and guaranteeing data availability and investigative support are a few of the suggested solutions to lower these risks (Tiwari and Pangerkar, 2024; Mallisetty et al., 2023). To create cutting-edge security procedures and cloud system solutions, cross-sector collaboration is crucial (Aijaz et al., 2024).

Furthermore, security concerns that affect several tiers of the cloud infrastructure, including hosts, data, networks, and applications, are a top concern even though cloud computing may offer services that are both scalable and reasonably priced. Its widespread use is constrained by these problems (Alghofaili et al., 2021; Chaudhari et al., 2023). Furthermore, multi-tenancy, another essential component of cloud computing, is very difficult to implement at all architectural levels. Data loss, unavailability, and privacy breaches might result from this (Alghofaili et al., 2021). Scientists have developed several remedies to deal with them,

including multi-factor authentication (MFA). However, there are still a lot of issues that need to be fixed, including cloud-related issues like flexibility (Alghofaili et al., 2021). Research is still being done to provide efficient security solutions to safeguard user and application data in cloud-based environments (Chaudhari et al., 2023). These security and privacy concerns must be addressed due to the increasing popularity and expansion of cloud use. However, the combination of cloud infrastructure with the Internet of Things adds another layer of complexity (Alghofaili et al., 2021).

2.4 Cloud Computing in IoT

Cloud computing and the Internet of Things combine to provide potent applications. As a result, IoT devices produce a lot of data that the cloud can gather, store, and analyze. Better decision-making, real-time monitoring, and sophisticated analytics are made feasible by this integration (Almutairi and Sheldon, 2025).

Because many IoT applications have strict latency requirements and limited resources, the authors of Aslanpour et al. (2020) made this point, stating that IoT environments need more advanced orchestration mechanisms than cloud systems. Edge and fog computing bring computational power closer to the end users and IoT devices to overcome communication delays and meet the real-time applications demands. These paradigms reduce latency, increase data locality, decrease bandwidth usage and promote privacy preservation. The two terms sometimes get used interchangeably, but they differ when it comes to a deployment of architecture. While fog computing normally places distributed computing resources between the cloud data centers and the end devices, edge computing actually computes on or in the vicinity of the IoT devices. While both paradigms have merits, they also have a number of limitations concerning limited computation resources, limited energy supply, and dynamic resource management. The emergence of edge-specific tactics like resource sharing and work offloading in these distributed environments exacerbates the issues caused by the additional computational layers.

The integration of cloud computing with the Internet of Things is systematically discussed in the paper by Nazari Jahantigh et al. (2020). After giving some background information on each of these technologies, it starts the process of combining them. The 38 chosen papers are divided into three categories: applications, platforms, and interaction with other technologies. They discuss advantages, including scalability and real-time analytics. Nonetheless, it recognizes persistent issues with standards, privacy, security, and effective resource management. Despite its usefulness, the study does not provide a critical evaluation of the advantages and disadvantages of the tactics covered in the example articles. Furthermore, the selection method itself has not been made completely accessible, and the coverage seems to be mostly restricted to recent years, leaving out significant contributions from earlier years. Despite being broad, the results do not offer any particular suggestions. The notion of IoT-cloud integration is finally covered in the work, but it would be helpful to expand and make it more thorough to include the evaluation of earlier studies.

Furthermore, the growth of cloud computing and IoT devices has resulted in a number of constraints at the moment, especially in the area of security. Hybrid systems are significantly more difficult to secure because of the variety of IoT devices and resource constraints. This makes it challenging to properly apply basic cloud protection procedures. Furthermore, problems like insider threats, virtualization vulnerabilities, and information breaches become even more prevalent as IoT data is moved to cloud settings. Additionally, the absence of unified systems to address both IoT and cloud-specific risks demonstrates a huge gap, as most solutions concentrate on a single element without taking into account a comprehensive security plan. This failure emphasizes how innovative and tested solutions are needed to address the additional security issues in this integration. According to Tawalbeh (2020) and the General Data Protection Regulation (GDPR) (De Marco, 2019), the answer to these issues is to have

strong security measures and raise user awareness so that they understand and abide by the aspects of the new technology that give them a sense of security.

2.5 IoT and Cloud Integration Security Studies

The challenge of safeguarding such systems is made more difficult by the scarcity of resources, the vast amount of data produced by IoT ecosystems, and the wide range of device kinds. Cloud system security issues are exacerbated by vulnerabilities brought on by a virtualized environment, insider threats, data breaches, and insecure APIs (Surianararayanaraja and Chelliah, 2023).

Data security, network and service security, application security, and human-related issues are the four main security challenges in IoT-enabled cloud computing. Since traditional security systems frequently fail, new strategies are needed, such as the application of deep learning and artificial intelligence (Ehsan Bazgir et al., 2023). Additionally, a shared responsibility paradigm between cloud service providers and IoT customers is necessary to optimize security in cloud-based IoT (Surianarayanarayan and Chelliah, 2023). The integration of security operations centers (SOCs) in IIoT systems and the investigation of open-source platforms are the current activities in this field (Ferencz et al., 2024). To handle these issues, a thorough strategy that incorporates secure service discovery, on-device credential security, and network anomaly identification is needed (Hossain et al., 2024). Industries should prioritize the usage of cloud computing, robust cybersecurity systems, and data collection techniques (Ferencz et al., 2024).

One of the most recent comprehensive studies looked at the security and privacy implications of IoT and offered a number of solutions, including privacy preservation and robust encryption techniques. However, it did not adequately address the cloud-specific security issues that arose in the context of cloud and IoT integration (Tawalbeh et al., 2020). Sharma also conducted an investigation of security issues in IoT scenarios, identifying several threat categories and mitigation strategies. However, it ignores the most recent dangers, such as malevolent assaults on cloud-based and IoT systems driven by AI (Shaukat et al., 2021). Abdur also provided a thorough examination of the security risks, weaknesses, and countermeasures in relation to IoT security. However, Abdur did not provide much information about low-power cryptographic techniques that are crucial for IoT devices that connect to cloud settings (Abdur et al., 2017).

According to the review of previous research, IoT and cloud security have both made significant advancements in their own fields, but the integration of the two has not received much attention. The threat of adversarial AI, the absence of lightweight encryption solutions, and a security framework are some of the major shortcomings.

3. Methodology

3.1 Research Design

This research uses a structured literature review approach along with qualitive case study analysis to explore the integration of Internet of Things (IoT) and cloud computing. The objective of the review is to integrate the key findings of recent research on IoT–cloud integration and to highlight the key characteristics of the systems (performance, security, privacy, scalability, and emerging distributed computing paradigms). Moreover, representative case-studies are analyzed to demonstrate how IoT–cloud architectures are implemented in practice and to assess their impact on performance and security in real-life environments.

3.2 Data Sources and Search Strategy

The literature search was done on the leading scientific databases like IEEE Xplore, Science direct, Springer link, Scopus, and MDPI journals that covers all the research areas related to cloud computing, Internet of Things, cybersecurity, distributed computing, and artificial intelligence.

To retrieve relevant studies, combinations of the following keywords were used: "Internet of Things (IoT)," "Cloud Computing," "IoT-Cloud Integration," "Edge Computing," "Fog

Computing," "Performance Evaluation," "Latency," "Scalability," "Energy Consumption," "Security," "Privacy," "Artificial Intelligence," and "Real-Time IoT." Boolean operators (AND/OR) were used to narrow down the search and promote the relevance of the retrieved publications.

3.3 Study Selection Criteria

The focus of the review was on publications from the last seven years, 2018 to 2025, which shows the rapid developments of IoT-cloud integration, edge and fog computing architectures, and AI-based security mechanisms. Only studies published in 2012–2017 that presented foundational concepts or reference architectures or adopted security models that are broadly used for security research were included in the earlier studies.

This included the following criteria:

- Journal articles and conference papers written by other researchers.
- Publications in English.
- Research on IoT-cloud integration, cloud, edge, fog computing, cybersecurity, privacy, interoperability, or AI in IoT.
- Studies that contain technical analysis, comparative analysis, implementation framework or comprehensive review results.

Exclusion criteria were:

- Duplicate publications.
- Non-peer-reviewed documents.
- Any articles that are not directly related to IoT-cloud integration.
- Research that does not have adequate technical or scientific contributions.

3.4 Literature Selection

Sixty-four (64) references were retained for this review after applying the selection criteria. Special attention was given to the latest and most relevant research focusing on cloud computing performance, edge and fog computing, cybersecurity, privacy protection, and artificial intelligence methods for IoT applications. The Results and Discussion section are based mainly on these studies.

3.5 Data Analysis

Qualitative comparative analysis approach was used for analysis of the selected studies. Several metrics were applied during the evaluations of each publication such as latency, scalability, energy consumption, reliability, security mechanisms, privacy protection, interoperability, resource management, and real-time processing capability. The results were then consolidated and analyzed to discuss the advantages and disadvantages of cloud, edge and fog computing architectures to find the common research trends, discuss the unsolved technical issues and suggest further research directions to improve the IoT-cloud integration.

3.6 Case Study Analysis

For complementing literature review, two representative case studies, namely, Smart Infrastructure and Smart Healthcare were analyzed to show practical implementations of IoT–cloud in the real-world scenarios.

Each case study was assessed on a number of technical criteria; these were not limited to descriptive examples and included:

- Response Time
- Scalability
- Reliability
- Security
- Privacy
- Overall System Performance

This analysis is designed to make the connection between the practical applications and the performance and security issues raised in the course of the review.

3.7 Comparative Evaluation

Finally, the results from the literature review and case study analysis were combined and compared the three technologies (Cloud Computing, Fog Computing, Edge Computing) in terms of latency, scalability, energy consumption, security, deployment cost, reliability, and suitability for real-time IoT applications.

The comparisons result in a complete picture of the advantages and disadvantages of each computing paradigm and facilitate the discovery of future research opportunities to enhance IoT–cloud ecosystems.

4. Results and Discussion

4.1 Results

The majority of IoT businesses use a variety of IoT framework technologies to manage sensors and send and receive real-time data. It is possible to measure and regulate variables like temperature, humidity, shocks, and vibrations while a product is being transported. Given that there are several advantages to integrating IoT with cloud computing, its use across a range of sectors can subsequently significantly improve resource efficiency and increase production capacity (Table 1). However, several obstacles must be overcome to deploy the IoT (Nam et al., 2022). Processing and analyzing vast volumes of data gathered by several sensors is one of the difficulties (Bauer and Aschenbruck, 2018). Furthermore, processing all of this collected data straight to a central server is inefficient and occasionally impractical owing to limited computer, network, and storage capacity, as well as overall power, prices, and unpredictable latency. To address these problems, the idea of an IoT cloud platform that moved data processing responsibilities to the IoT Cloud was introduced.

Table 1 *Benefits of integrating IoT and cloud technology*

IT Infrastructure Flexibility and Scalability	Economy of Cost
Two important advantages of integrating cloud and IoT technologies are scalability and flexibility. Businesses have changed as a result of IoT devices producing massive amounts of data. Depending on demand, corporate organizations may quickly scale up or down thanks to cloud technology. Additional flexibility is offered by cloud computing, which makes data and applications accessible from any location.	Businesses may save money by implementing cloud computing and IoT. Businesses may quickly save a significant amount of money on infrastructure while still having access to scalable storage and data analytics capabilities thanks to the cloud-based platform. Additionally, the automated procedures result in lower starting costs and higher operational effectiveness.
Enhanced Security of Data	Enhanced Dependability and Performance
In the current digital age, data security is a significant concern, and cloud and IoT technologies contribute to its improvement. Private information that devices exchange over a network can be protected using Transport Layer Security (TLS) and other encryption techniques. Furthermore, the likelihood of insider threats and privileged access abuse will be reduced by implementing role-based access control procedures and multi-factor authentication.	Cloud computing and the Internet of Things, when combined, may help organizations become much more reliable and efficient. This combination enables the real-time data to be analyzed and used more quickly, resulting in actionable insights to help make better decisions. For IoT devices to consistently send the correct data, they need quick and effective communication. Because cloud computing offers rapid access to the same data and affordable storage space, the data is made available when needed.

4.1.1 Case studies

According to Mohammed Sadeeq et al. (2021), cloud computing services are used by a number of IoT-related industries, including education, augmented reality, manufacturing, emergency recovery, smart cities, remote forensics, hospitality, e-government, human resources, and the Internet of Cars. The Internet of Things, cloud computing, and associated application settings provide certain unique issues (Shukur et al., 2020).

4.1.1.1 IoT–Cloud Performance Challenges in Smart Infrastructure

The study uses a cloud computing application to examine IoT-based infrastructure in Kyiv, Ukraine, in the context of public transportation systems. Cloud computing is a component of the server infrastructure of intelligent public transportation systems. As the needs and complexity of contemporary transportation increase, there is a good chance that the adoption of the Internet of Things idea will improve passenger comfort and efficiency. Because the demand created by IoT devices is unexpected and dynamic, traditional infrastructure (with dedicated servers) is not the best option. The research by Zakutynskyi I. (2023) also considers the fact that cloud computing will be the primary server infrastructure for the aforementioned systems. The authors created the overall system design and assessed the performance and scalability of each server infrastructure component separately.

A software emulator that mimicked the controller module found in automobiles was created to test the system. Stress tests were conducted using the created emulator to verify and validate the suggested architecture's capacity to handle and scale input data. The test scenarios were developed and carried out using Kyiv, Ukraine's current public transportation system as a base. The experiment's findings demonstrated that the proposed IoT architecture can be effectively scaled to handle the load generated by the linked devices. A stable system functioning is shown by the fact that the average time to process a message and the error rate do not increase as the number of incoming messages increases between 40 and 6000. The findings may be applied to both the development of new public transportation systems and the modernization of existing ones.

Performance Challenges

Cloud computing outperforms IoT devices and network edge infrastructure in terms of computation and storage. However, cloud-based IoT is not a practical option for a variety of applications due to intrinsic limitations (inadequate network latency, lack of location awareness, security and privacy concerns, etc.). On the other hand, edge computing lowers latencies, but it does not ensure an end-to-end response time; instead, it fixes it through computation time (Bulej et al., 2021). As a result, to meet the increasing demands of IoT applications, a parallel computing paradigm will be needed (Hu et al., 2017). According to some experts, the post-cloud age is already upon us (Mass et al., 2020). By bringing basic compute functions (filtering and basic data processing) closer to the IoT devices (data source), computing paradigms including edge computing, fog computing, MEC, MCC, and cloudlets assist address some of these problems. They make it possible to calculate data in real time without transferring it to the cloud. In contrast to our conventional IoT-Cloud architecture, the method lowers network latency (Farris et al., 2018). The filtered and condensed data can be moved to the cloud in the event that a big volume of data requires more sophisticated processing and storage. However, depending on the needs of the particular IoT application and the state of the system resources, all offloading methods face a variety of difficulties.

According to Aslanpour M. S. (2020), edge and fog computing may be used to meet the latency requirements of the Internet of Things-based application while lowering the overall delay. However, orchestration faces additional difficulties and variations with fog and edge, including unstable supplies and restricted energy. The incorporation of edge-specific techniques,

including resource sharing and task offloading in these distributed contexts, complicates the differences and adds additional issues due to the additional layers of computerization.

Applied Solutions

To achieve some of the objectives, orchestration development efforts must be carried out. According to the literature, the current solutions are meant to achieve a number of goals, including cost and delay reduction, energy control, and more (Gill and Buyya, 2019). For example, the authors of Aslanpour et al. (2019) use a dynamic resource provisioning technique to try to improve gaming apps and lower latency. For latency-sensitive applications, a number of these strategies were created with energy as the goal (Chou et al., 2019). Both the service's goals and its stakeholders are diverse.

Performance Analysis

The smart infrastructure case study illustrates the potential of cloud-enabled IoT solutions to effectively operate large-scale urban services, such as transportation, energy distribution, and public utilities. The main challenge is to ensure low response latencies even for large amounts of data generated by sensors. Scalability is crucial, given the continuous growth of smart city environments with the deployment of more IoT devices. Distributed computing architectures, like fog and edge computing, can minimize the chance of single points of failure, increasing reliability. The basic security elements are essential for the protection of critical infrastructure from cyber threats, while privacy mechanisms are needed for the protection of citizen-related information. As a result, it has been shown in this case study, that optimizing performance, increasing cyber security and protecting privacy are all important factors to consider when deploying smart infrastructure successfully.

4.1.1.2 Case Study: IoT–Cloud Security Challenges in Smart Healthcare

IoT-enabled connected medical devices are becoming more and more important in the healthcare industry for processing and tracking patient health. To deliver real-time diagnostic and treatment suggestions, smart healthcare systems make use of wearable sensors, cloud-based electronic health records (EHRs), and remote patient monitoring (RPM) devices. Sensitive medical data is gathered by these Internet of Things devices, then sent to cloud platforms for analysis and storage. However, there are serious security issues with IoT and cloud services since patient data is susceptible to cybercrimes (Almutairi and Sheldon, 2025).

Security Risks in Smart Healthcare

Data breaches: Sensitive patient information will be made public if unauthorized access to EHRs is made possible by dangerous APIs or inadequate authentication procedures. Between 2010 and 2019, hacking and IT incidents were shown to be the most common causes of healthcare data breaches, with a noticeable rise in recent years (Seh et al., 2020).

Replay attacks: Medical IoT devices, such as pacemakers and smart insulin pumps, can only be remotely configured and monitored over a wireless link. Replay attacks, in which a hacker pauses and repeats earlier commands, altering medication dosages or turning off life-saving equipment, have the potential to be lethal. Wireless infusion pumps have been shown to have vulnerabilities that can be taken advantage of (Mejia-Granda et al., 2024).

Adversarial AI attacks: Several healthcare systems utilize AI-informed diagnostic models to identify medical disorders based on sensor data. An attacker can fool AI models into making the wrong diagnosis and prescribing the wrong treatment by manipulating input data, such as blood glucose levels and ECGs. According to research, adversarial assaults on medical image classification systems can result in a patient's misdiagnosis, which can seriously jeopardize their health (Tsai et al., 2023).

Applied Security Solutions

To lessen these security risks, smart healthcare has turned to several IoT-cloud security solutions, which include the following:

Cryptography that is lightweight: Since medical IoT devices have limited resources, lightweight encryption algorithms like PRESENT and ECC are utilized to preserve data privacy. These algorithms also require very little electricity. Lightweight cryptographic solutions are required because IoT healthcare security flaws in both software and hardware have been shown to endanger patient security and system integrity (Mejia-Granda et al., 2024). Rate capping, API gateways, and OAuth 2.0 authentication are some of the strategies used to prevent DoS attacks and illegal access to healthcare APIs. Studies show that APIs in healthcare IoT systems require a high level of security in an effort to stop illegal access and information leakage (Al-Rumaim and Pawar, 2023).

AI-based IDS: machine learning models keep track of IoT device activity and identify anomalies in data transfer that might point to an attack, including replay attempts or malevolent AI manipulations. As a result, deep learning methods might be useful for spotting threat patterns and protecting IoT healthcare networks.

Performance Analysis

Overall, the smart healthcare case study highlights the benefits of combining IoT devices with cloud computing in improving remote patient monitoring, accessibility of medical data, and healthcare service continuity. But there are also performance issues with the architecture. The delay in responding to the emergency may cause the clinical decision to be delayed in such cases, where cloud-based processing is more involved. The scalability is still another major benefit which allows healthcare service providers to accommodate a growing number of medical devices and patients that are connected. Cloud redundancy enhances service availability but can also introduce a requirement for stable network connections, potentially impacting system resilience. Medical data is highly sensitive and processing it demands robust authentication, encryption, and adherence to regulatory compliance, which makes security and privacy paramount. The overall case shows the importance of balancing the real-time response with strong security and privacy measures to achieve high system performance.

4.1.1.3 Key Findings

Although IoT-cloud security has advanced, security issues with smart systems, smart infrastructure, and smart healthcare still pose a serious threat. Finding a balance between security and hardware limitations is one of the most important concerns in the case of IoT devices. This makes it challenging to guarantee the use of robust cryptographic security. Recent studies highlight the necessity for enterprises to self-assess cybersecurity in order to successfully address operational security restrictions (Burke et al., 2024). When quantum computing is developed, the company will become obsolete, which is why PQC is crucial for data security. Although there is a dearth of specialized studies on PQC in IoT, researchers stress the significance of creating quantum-resistant security mechanisms (Li et al., 2023). Implementing a zero-trust security paradigm, which requires all users and devices to verify themselves before they can access cloud services, can also lessen the risk of unwanted access. According to the research, zero-trust security may greatly improve the strength of IoT integration with clouds (Sarkar et al., 2022).

To improve data protection and make sure that IoT-cloud-based services are resistant to emerging cyberthreats, systems might incorporate the following security measures. These examples are included in our analysis because they provide credence to the further integration of IoT into cloud security frameworks. It also emphasizes how urgently additional study and flexible security solutions are needed.

4.2 Discussion

4.2.1 IoT and Cloud combining Performance Challenges

Regarding the domain in which they are used, cloud computing and the Internet of Things each have their own problems. The main issue with cloud computing is security. High-level

authentication and encryption procedures are necessary to protect sensitive data since cyberattacks on vast volumes of data stored on distant servers are feasible. Furthermore, it is crucial to guarantee the continuous availability and dependability of cloud services, which calls for appropriate infrastructure architecture and redundancy to avoid any outages (Shukur et al., 2020). Conversely, the incompatibility of devices from various manufacturers is a problem for IoT. Because many systems and equipment are connected using different protocols and standards, there is a compatibility issue that makes communication difficult.

Furthermore, as IoT devices frequently run on low power, energy efficiency is a crucial factor to take into account in order to extend battery life and ensure continuous operation. To fully realize their potential (address these inherent problems), cloud computing and IoT ecosystems will require constant innovation in the areas of security protocols, standardization initiatives, and energy-efficient designs (Table 2). The use of cloud computing integration with the Internet of Things has presented several obstacles and produced a range of results. Given how they impact and complement one another, the recent, rapid worldwide deployment of cloud computing and IoT holds significant promise (Ishaq et al., 2021). Numerous cloud and Internet of Things researchers have envisioned applications to collect and process data utilizing computer processing and cloud storage.

Table 2 *Performance Challenges in combining the IOT and cloud technology and its solutions*

	Challenges	Solution
Network Latency	Network latency delays in information flow between devices are a significant problem in an environment where cloud computing and the Internet of Things have been combined. As more IoT devices are able to communicate with the internet and send data to it, latency issues might arise. Faster processing and storage are two possible benefits of cloud computing. Network latency may still have an impact on the distance between IoT devices and network servers, though.	Edge computing of data close to the IoT device can be used to reduce latency. By lowering the protocols used for communication between IoT devices and the cloud, latency may be decreased in places with poor connectivity or bandwidth.
Interoperability	One of the main challenges to IoT and cloud computing integration is interoperability. The two systems' different data formats, security requirements, and communication protocols are the root of the issue.	Standard protocols and rules for data sharing between cloud computing resources and Internet of Things devices hold the key to fixing such issues.
Power	Since IoT devices frequently run on low power, energy efficiency is essential to extending battery life and ensuring device dependability. An even higher level of power consumption will emerge when cloud connections and IoT networks spread around the world because of the increased volume of data being transmitted. It is difficult to imagine a world where billions of	Energy-efficient solutions should be continually improved to reach their potential in order to overcome these fundamental problems in cloud computing and IoT systems. Installing self-sustaining power-generating systems would also be necessary since the devices would need to be powered by

	sensors and low-power gadgets would work together. A reliable power source and an appropriate energy use system are necessary in such a setting.	the environment in order to provide the necessary amount of energy.

Table 3 *Comparative Performance Analysis of Cloud, Fog, and Edge Computing*

Evaluation Metric	Cloud Computing	Fog Computing	Edge Computing
Latency	High due to remote processing	Medium	Very Low
Energy Consumption	High in communication	Medium	Low
Scalability	Excellent	Good	Moderate
Security Level	High with centralized security controls but vulnerable to cloud-targeted attacks	Good with distributed protection mechanisms	Moderate; depends on device capabilities
Deployment Cost	Moderate	High	Moderate
Suitability for Real-Time IoT Applications	Limited	Very Good	Excellent

The findings presented in the literature reviewed are summarized in Table 3, and provide an overview of the comparative characteristics of the three architectures. While cloud computing provides excellent scalability and centralized resource management, it does have some drawbacks of relatively high latency because of the physical separation between IoT devices and cloud data centers. Fog computing brings computation resources closer to the network edge, while edge computing is the closest to the edge and is ideal for time-sensitive IoT applications. Generally, though, edge devices have smaller computational power than cloud infrastructures. Thus, the choice of architecture will depend on the type of application, especially for latency, scale, security, energy use and deployment expenses.

4.2.2 IoT and Cloud Combining Security Challenges

Data Privacy Issues :Data privacy issues arise when cloud computing and IoT are combined. Sensitive information sent to the cloud by IoT devices increases the likelihood of illegal access and data breaches. Data transfer via sensors or other devices may lead to undefined data processing and a loss of privacy.

A lot of private data is also collected by IoT devices and sent to cloud servers for analysis and storage. Access control and data encryption are necessary to guarantee the security of this information and prevent unauthorized access. Furthermore, the authentication and authorization systems must be strong enough to help identify the identities of both people and machines linked to the IoT system through the cloud, as weak authentication can lead to security breaches and information leaks (Albshaier et al., 2024).

Without proper validation and integrity checks, data between devices and the cloud may be subject to alteration or manipulation, which might compromise the data's correctness and dependability. This is the other major security concern. In order to prevent unwanted data interception, MitM attacks, and spying, it is crucial to ensure the security of the bridges between cloud servers and IoT devices. This makes network security a top priority as well. To prevent such risks to network security, encryption technologies and encrypted communication channels can be installed (Lee and Lee, 2021).

The problem of data privacy can be resolved with the help of the Internet of Things. All of that calls for appropriate security measures to guarantee that data stored in the cloud is safe from assaults and unauthorized access. The risks are increased when using third-party data centers, particularly when inadequate security is present. The security of the IoT devices themselves is also a big worry since, typically, they have little memory and processing power, making them vulnerable to security threats like malware and illegal access. By doing this, it will be necessary to implement strong security standards and continuously update equipment with security updates in order to prevent any vulnerabilities. Good security, regular audits, emergency response in the event of an attack, and knowledge of new cloud and IoT risks should all be part of the overall strategy for addressing these security issues (Lee and Lee, 2021). IoT-cloud integration can improve data security only when appropriate protection mechanisms are implemented, such as encryption, multi-factor authentication, access control, and continuous monitoring. However, this integration also increases the attack surface and introduces new cybersecurity risks.

4.2.3 Evaluation of Current Security Solutions

One of the most important aspects of the growth of the IoT ecosystem with cloud computing is the ability to analyze data on demand and the potential for scalable resources. The greatest option for processing, storing, and analyzing the massive amounts of data produced by IoT devices is provided by cloud systems. However, the majority of current solutions are still unable to address the particular security issues raised by cloud-based systems, particularly when combined with the Internet of Things (Almutairi and Sheldon, 2025).

Maintaining data integrity, privacy, and secrecy in a multi-tenant system is another important cloud security challenge. IAM solutions were created to solve these issues, but they are still unable to manage the growing number of IoT devices and data streams and produce consistent access control policies in heterogeneous contexts. Recurring IAM solutions are vulnerable to insider threats and insecure APIs, and they are unable to safeguard cloud orchestration systems that access and manage cloud resources (Gibson et al., 2012). IoT-cloud systems, where resource-constrained devices and resilient cloud infrastructures combine to form a complicated attack surface, may be even more vulnerable.

Isolation, data breach, and service failure are additional hazards associated with cloud systems' multi-tenancy feature. When several tenants (such as IoT service providers and consumers) share a cloud infrastructure, there are a number of things to take into account. The cloud's flexibility limits the currently proposed solutions, such as MFA, which results in varying security applications for various services. Blockchain-based identity management has been explored in relation to safe access control and decentralized authentication in order to lower the risks. The research of current attack trends can help enhance the identification of cloud threats based on AI-powered security surveillance. To solve the issues of cross-tenant security and dynamic cloud workloads, these technologies need to be further enhanced (Almutairi and Sheldon, 2025).

It is not frequently recognized that blockchain technology may be used in conjunction with IOT to improve the security and trust of a variety of applications. However, the integration also brings with it certain new cybersecurity problems that must be resolved. In order to counter these cybersecurity risks, the asset is required due to the improved degree of security and resource scalability provided by cloud computing. One of the most important cybersecurity considerations when integrating IoT with blockchain is the safe processing and storage of massive amounts of data produced by IoT devices. Cloud storage can offer data security and integrity while storing this data in a scalable and safe environment (Albshaier et al., 2024).

Furthermore, by providing a robust infrastructure for the deployment of blockchain nodes, the idea of cloud computing may be utilized to improve the security of blockchain networks. Cloud-based blockchain solutions might improve network availability and scalability, reduce

the danger of single points of failure, and boost security in general. Advanced cloud security features like encryption, access control, and monitoring may be used to offer an extra layer of protection to blockchain data and transactions. A secure connection between IoT devices and blockchain networks can also be established by utilizing cloud-based IoT gateways, which could be regarded as an assessment that would guarantee data transfer and authentication between the IoT devices and the blockchain nodes. Additionally, blockchain enhances Internet of Things networks' transaction monitoring and transparency. The blockchain provides a visible and auditable record of every transaction and data exchange. Real-time surveillance and reporting of suspicious activity or abnormalities will be facilitated by this type of openness (Park & Park, 2017).

However, security may be threatened by the interconnection of blockchain, cloud, and IoT. One of the potential security dangers may be the intricacy of managing a hybrid system that combines blockchain, cloud, and IoT technologies, each of which has unique security needs and weaknesses. The use of blockchain is another challenge, which calls for reliable consensus methods and safe smart contract implementations. According to Albshaier et al. (2024), providing equal security on all three levels is a challenging undertaking that requires a complete approach to ensure successful administration and monitoring of each component's security status.

4.2.4 IoT–Cloud Integration and Emerging Directions

New study fields, particularly in security, have been brought about by the integration of cloud systems with the Internet of Things. Because IoT devices are frequently located in varied and resource-constrained areas, traditional cloud security techniques like encryption and access control may not always be appropriate. One way to get around these issues is to use lightweight cryptography. Algorithms like ECC and lightweight ciphers like PRESENT, SIMON, and SPECK are being investigated to guarantee the security of the communication process and to lessen the strain on the already constrained resources of IoT devices (Tan and Samsudin, 2021).

Despite its potential, lightweight encryption still faces a major scaling issue. IoT, and especially IIoT, has many industrial applications that need real-time processing and minimal latency. The conventional encryption methods, such as RSA and AES, need a lot of resources for Internet of Things devices and are not scalable to large-scale applications. This problem is especially important in IIoT systems where security and quick decision-making are necessary. For IoT systems, lightweight cryptography techniques have to be such a balance between preserving high security and reaching the ideal degree of efficiency. As the IoT ecosystem grows, further research on hybrid cryptography designs—which blend standard and lightweight encryption—can provide additional scalability options (Almutairi and Sheldon, 2025).

Furthermore, recent studies have concentrated on how AI may improve cloud and IoT security. AI and IDS-based IoT anomaly detection have shown promise in spotting questionable activities in an IoT network. However, the use of AI models in IoT-cloud systems carries a serious danger of being attacked by adversaries. Evasion, poisoning, and model inversion are attack types that can impact AI model performance because they allow hackers to get past detection measures and take control of IoT devices covertly. Future studies should concentrate on strengthening AI models against malevolent attackers using techniques like adversarial training and robust optimization. Furthermore, blockchain and artificial intelligence (AI), in conjunction with safe data sharing and verification in the form of decentralized and impermeable systems, can significantly improve security (Almutairi and Sheldon, 2025).

The Search for Uniform Solutions to All Security Challenges demonstrates the necessity of global cybersecurity given the explosive rise of IoT devices. Individual countries have created unique legislative laws in an effort to improve IoT security. The creation of laws like the Cybersecurity Act and Cyber Resilience Act, which supplement the Network and Information Security Directive and GDPR, was part of the EU's efforts to strengthen cybersecurity.

Similarly, the Federal Trade Commission Act, Cybersecurity Information Sharing Act, and COPPA are other IoT regulations in the United States (Lata and Kumar, 2021). Other nations have laws that apply to their own nations, and other nations are currently creating regulations. Despite national IoT rules, there is a global demand for a uniform security solution and certain related ongoing initiatives. Approaching the issue is challenging due to the large number of security and privacy issues with cloud-based IoT and the absence of a generally applicable security solution. Several productive industrial collaborations are in progress to accomplish this. Having standardized verification methods that are tailored to balance security and usability across all IoT categories is, therefore, a viable option, even though the implementation is still difficult for all IoT categories. The differences between the two categories of IoT devices—traditional and cloud-based—support this (N. Singh et al., 2024).

It should make it easier to integrate blockchain and artificial intelligence and to put in place a multi-level protocol verification scheme tailored to the Internet of Things. This scheme should pay particular attention to stringent security checks at the manufacturing, cloud, and third-party service levels. The strategy will provide a methodical and uniform security assessment procedure. To deliver IoT categories with more stringent resource limits, like AIoT, we suggest using machine learning-based adaptive verification systems. These systems' scalability may lead to successful deployment by enabling the dynamic application of security measures based on real-time device usage patterns. Depending on how complicated the devices are, large-scale IoT eco-systems and AI-controlled modular verification systems may change the security procedure. Giving manufacturers and cloud providers incentives or certification for using the same might further encourage adoption. Therefore, we think that a standardized verification procedure like this might be a big step in the right direction for resolving security issues, especially when it comes to life-critical IoT products.

Finally, Results from this review suggest that cloud computing remains the core of IoT ecosystems, offering flexible storage and computational power. But the need for ultra-low latency, real-time responsiveness and distributed intelligence shows that many today's IoT applications cannot be fulfilled by a cloud-only approach. The emergence of new paradigms like edge and fog computing that can process delay-sensitive tasks nearer to end devices are not intended to "take over" cloud computing, but are intended to supplement it. Thus, future IoT systems are anticipated to take the form of HCEF (hybrid cloud–edge–fog) architectures that combine the benefits of all three computing paradigms while overcoming each individual's shortcomings.

5. Study limitations

In this research, there are several limitations that are acknowledged, which could interfere with the interpretation and application of the study in a wider context. To begin with, there can be some prejudices in the choice, availability, and scope of the considered sources since the study primarily involves the use of secondary data, including case studies and academic articles. The absence of primary empirical data is likely to affect the explanatory power of the study as far as the practical issues and user experiences are concerned, because this limits the ability to test theoretical concepts on actual empirical or survey data.

Second, relying excessively on the recently published material can omit important yet older background research or newly accessible unpublished information that could provide a more complete picture of the IoT-cloud integration. The currently available research is mostly global or even regionally generalized, thus restricting geographic scope and failing to fully consider the regional disparities in technology infrastructure, the legislative context, or the cultural factors influencing adoption and security processes.

Third, it has time constraints because IoT and cloud computing technical environments are evolving rapidly. The solutions and issues covered by the study would become outdated as

breakthroughs or standards are adopted, particularly in security measures and architecture. This time limit affects the long-term utility of some of the results.

To reduce such limitations, future research may incorporate longitudinal empirical research designs that employ an array of industrial and geographic settings to capture both qualitative user experience and quantitative performance indicators, using a mixture of methods to capture both. The standardized frameworks and real-time monitoring of new technologies would also be stronger in future assessments. The relevance and strength of the IoT-cloud solutions would be enhanced globally in the event that the research remit is broadened to include the local regulations and infrastructure. This would allow making more context-specific proposals.

In general, a better understanding of the challenges and the solutions related to the integration of IoT and cloud computing will be achievable with the help of a balanced type of approach that would involve the approaches to the theory and additional empirical data, and insights that would be specific to the context.

6. Research Gaps

When one critically examines the literature, it is evident that much has been achieved regarding the interactions between the IoT and cloud computing, mainly regarding scalability architecture, real-time data analytics, and security concerns. The ability of cloud service models to operate the volumes of IoT data has been researched extensively in the past literature, as well as issues related to latency, heterogeneity of devices, and interoperability. Moreover, it has been observed that progress in AI-based edge computing and thin security protocols offers promising solutions to long-standing limitations of the IoT.

However, the existing literature does still have serious gaps. To begin with, although security concerns are receiving high consideration, there is a lack of research on the unified, flexible security infrastructures capable of balancing the competing requirements of scalability, real-time responsiveness, and stringent privacy legislations within most countries. Contemporary studies often concentrate on the security aspect of discrete cases without considering a comprehensive approach that integrates updates to firmware, device management, and dynamic threat identification at the same time.

Second, all the research is concentrated on technological development, whereas the real role of implementing cloud-based IoT systems in various environments and, in particular, in the framework of organizations with fewer resources or other geographical locations is underreported. There is no empirical evidence about the influences of regulatory variances and infrastructural inequalities on system adherence and effectiveness that should be put into practice.

These gaps can be addressed by the study through an analysis of the security, interoperability, and operational issues that cloud-IoT ecosystems encounter. It can enhance the knowledge of comprehensive, versatile solutions that align with technology development and contextual, regulatory reality across the globe by synthesizing interdisciplinary knowledge and case studies of numerous areas. The opportunity to offer the frameworks and recommendations designed to enhance the system resilience, user confidence, and sustainable scalability is what makes the research have scientific and practical importance. This will assist in leading future technical developments and policy-making in this rapidly developing industry.

This specific study of these under researched areas eliminates important barriers to the safe and widespread implementation of IoT-cloud and gives space to the best designs that can support new applications in numerous fields.

7. Implications and Future Directions

The conclusions of the research have significant theoretical and practical implications for the field of cloud computing and IoT integration, which is still developing. The paper just helps to

better the theoretical understanding of the significance of cloud infrastructures in their ability to process the massive amounts of data generated by various IoT devices and address the severe security vulnerabilities. This contributes to the scholarly debate by highlighting the necessity of comprehensive, scalable frameworks that allow balancing scalability, real-time responsiveness, and privacy concerns in dynamic networks of the IoT-cloud environments.

In applied terms, the study assists in developing and adopting more resilient, effective, and adherent IoT-cloud systems through training the technology developers, system architects, and legislators on necessary significant security practices, architectural aspects, and operational issues.

The application of interdisciplinary concepts of cloud resource management, cybersecurity, and IoT systems contributes to the further development of knowledge and helps to approach new issues comprehensively. To enhance user confidence and stability in the system, it also outlines the importance of lightweight encryption, AI-based intrusion detection, and zero-trust security frameworks that can be applied in resource-limited devices. Moreover, the emphasis on practical case studies demonstrates the relevance and the situational peculiarities of proposed resolutions in such areas as smart infrastructure and healthcare.

The research in the future should aim more at developing universal and standard security structures that are capable of dynamically adjusting to threats and other regulatory settings around the globe. In order to expand latency and resource consumption, the interaction between multi-cloud systems and edge computing systems with IoT devices needs to be researched. Also, it can be empirically and long-term studies examining the practical effectiveness and acceptability of these technologies in most socioeconomic and geographic settings.

In a more methodological manner, further understanding of the system performance and user experience can be reached by expanding the empirical evidence with the help of mixed-methods research that integrates large quantitative data with qualitative information. There is a need to conduct longitudinal research to illustrate the impacts of rapidly evolving technology over time. In addition, future results would become more generalizable and applicable with the inclusion of a broader variety of types of IoT devices, industrial uses, and different geographic locations.

Moreover, the study will prove highly useful to other researchers in the future as they will have a good starting point in conducting their studies on this area. Future scholars may also use the findings of this research to explore the issue concerning security in more detail, with references to other applications and innovative methods of enhancing the security of cloud computing and interconnected IoT systems. The present work is significant as it could lead to a change in the direction of the safer, more effective, and more optimal application of these technologies in a variety of spheres. Finally, the conduction of this research is critical in ensuring that cloud computing and IoT integration proceed in a safe, reliable, and ground-breaking manner, driving progress and development in various sectors.

Conclusion

This review in detail and comprehensively explored the integration of Internet of Things (IoT) with Cloud Computing with a special focus on the technical challenges, performance considerations, security concerns, and new research trends that shape the success of contemporary IoT ecosystems.

The aim of this study was to identify the main challenges of the integration of IoT and cloud. The review has proven that latency, scalability, interoperability, energy consumption, and resource management are still the most challenging issues of performance in the IoT enabling cloud environment, and cybersecurity, privacy preservation, authentication, encryption and secure data management are the most critical security-related concerns.

The second goal was to analyze the support provided by the various computing paradigms for IoT applications. The comparative study showed that traditional cloud computing offers superb scalability and computing power, while real-time applications also have the limitation of communication latency. Fog and edge computing, on the other hand, can greatly enhance response time, decrease bandwidth usage and boost local decision-making, fitting them for latency-sensitive IoT services.

The third goal was to explore existing technologies and solutions presented to overcome these challenges. Based on the literature reviewed, AI, federated learning, lightweight cryptography, blockchain, and ZT architectures are found to be promising solutions for enhancing the system performance and cybersecurity. However, finding an optimal combination of performance efficiency, scalability, security and privacy continues to be an open research question.

In addition, smart infrastructure and smart healthcare case studies analysis showed that robust security mechanisms, efficient real-time processing and scalable computing resources are crucial for a successful deployment of IoT–cloud. These practical applications verified that system performance and cyber security are not mutually exclusive goals for design, but are complementary.

The overall conclusion of this review is that the IoT–cloud ecosystem of the future will increasingly rely on intelligent distributed computing architectures that combine cloud, fog, and edge computing techniques with intelligent and adaptive ability to manage resources and security services via AI. For this reason, further studies on building comprehensive frameworks that simultaneously optimize performance, security, energy efficiency, and privacy for the increasing complexity of big-scale IoT applications are suggested.

References

Abba Adamou, A. A., Ngangmo, O. K., Titouna, C., Thiare, O., Kolyang, Mohamadou, A., & Gueroui, A. M. (2024). Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges. Applied Computing and Informatics, 20(1/2), 119–141. https://doi.org/10.1016/j.aci.2019.11.005

Abdulazeez, D. H., & Askar, S. K. (2023). Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment. IEEE Access, 11, 12555–12586. https://doi.org/10.1109/ACCESS.2023.3241881

Abdur, M., Habib, S., Ali, M., & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. International Journal of Advanced Computer Science and Applications, 8(6). https://doi.org/10.14569/IJACSA.2017.080650

Aijaz, U., Abubakar, M., Reddy, A., . A., & C Pujari, A. (2024). An Analysis on Security Issues and Research Challenges in Cloud Computing. Journal of Security in Computer Networks and Distributed Systems, 1(1), 37–44. https://doi.org/10.46610/JoSCNDS.2024.v01i01.005

Albshaier, L., Budokhi, A., & Aljughaiman, A. (2024). A Review of Security Issues When Integrating IoT With Cloud Computing and Blockchain. IEEE Access, 12, 109560–109595. https://doi.org/10.1109/ACCESS.2024.3435845

Al-Dhuraibi, Y., Paraiso, F., Djarallah, N., & Merle, P. (2018). Elasticity in Cloud Computing: State of the Art and Research Challenges. IEEE Transactions on Services Computing, 11(2), 430–447. https://doi.org/10.1109/TSC.2017.2711009

Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Al-rimy, B. A. S. (2021). Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges. Applied Sciences, 11(19), 9005. https://doi.org/10.3390/app11199005

Almutairi, M., & Sheldon, F. T. (2025). IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. Electronics, 14(7), 1394. https://doi.org/10.3390/electronics14071394

Al-Rumaim, A., & Pawar, J. D. (2023). Exploring the Evolving Landscape of API Security Challenges in the Healthcare Industry: A Comprehensive Review. 2023 16th International Conference on Security of Information and Networks (SIN), 1–8. https://doi.org/10.1109/SIN60469.2023.10474998

Aslanpour, M. S., Ghobaei-Arani, M., Heydari, M., & Mahmoudi, N. (2019). LARPA: A learning automata-based resource provisioning approach for massively multiplayer online games in cloud environments. International Journal of Communication Systems, 32(14). https://doi.org/10.1002/dac.4090

Aslanpour, M. S., Gill, S. S., & Toosi, A. N. (2020). Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. Internet of Things, 12, 100273. https://doi.org/10.1016/j.IoT.2020.100273

Bauer, J., & Aschenbruck, N. (2018). Design and implementation of an agricultural monitoring system for smart farming. 2018 IoT Vertical and Topical Summit on Agriculture - Tuscany (IOT Tuscany), 1–6. https://doi.org/10.1109/IOT-TUSCANY.2018.8373022

Bruschi, R., Genovese, G., Iera, A., Lago, P., Lamanna, G., Lombardo, C., & Mangialardi, S. (2017). OpenStack Extension for Fog-Powered Personal Services Deployment. 2017 29th International Teletraffic Congress (ITC 29), 19–23. https://doi.org/10.23919/ITC.2017.8065705

Bulej, L., Bureš, T., Filandr, A., Hnětynka, P., Hnětynková, I., Pacovský, J., Sandor, G., & Gerostathopoulos, I. (2021). Managing latency in edge–cloud environment. Journal of Systems and Software, 172, 110872. https://doi.org/10.1016/j.jss.2020.110872

Burke, W., Stranieri, A., Oseni, T., & Gondal, I. (2024). The need for cybersecurity self-evaluation in healthcare. BMC Medical Informatics and Decision Making, 24(1), 133. https://doi.org/10.1186/s12911-024-02551-x

Chaudhari, A. R., Gohil, B. N., & Rao, U. P. (2023). A review on cloud security issues and solutions. Journal of Computer Security, 31(4), 365–391. https://doi.org/10.3233/JCS-210140

Chou, C.-H., Bhuyan, L. N., & Wong, D. (2019). μDPM: Dynamic Power Management for the Microsecond Era. 2019 IEEE International Symposium on High Performance Computer Architecture (HPCA), 120–132. https://doi.org/10.1109/HPCA.2019.00032

Čolaković, A. (2023). IoT systems modeling and performance evaluation. Computer Science Review, 50, 100598. https://doi.org/10.1016/j.cosrev.2023.100598

De Marco, G. (n.d.). Privacy Risk in the IoT Environment: the Need for a Multiple Approach According to the GDPR Principles.

Ehsan Bazgir, Ehteshamul Haque, Numair Bin Sharif, & Md. Faysal Ahmed. (2023). Security aspects in IoT based cloud computing. World Journal of Advanced Research and Reviews, 20(3), 540–551. https://doi.org/10.30574/wjarr.2023.20.3.2481

Farris, I., Orsino, A., Militano, L., Iera, A., & Araniti, G. (2018). Federated IoT services leveraging 5G technologies at the edge. Ad Hoc Networks, 68, 58–69. https://doi.org/10.1016/j.adhoc.2017.09.002

Ferencz, K., Domokos, J., & Kovács, L. (2024). Cloud Integration of Industrial IoT Systems. Architecture, Security Aspects and Sample Implementations. In Acta Polytechnica Hungarica (Vol. 21, Issue 4).

Fotouhi, H., Moreira, D., Alves, M., & Yomsi, P. M. (2017). mRPL+: A mobility management framework in RPL/6LoWPAN. Computer Communications, 104, 34–54. https://doi.org/10.1016/j.comcom.2017.01.020

Gibson, J., Rondeau, R., Eveleigh, D., & Tan, Q. (2012). Benefits and challenges of three cloud computing service models. 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), 198–205. https://doi.org/10.1109/CASoN.2012.6412402

Gill, S. S., & Buyya, R. (2019). A Taxonomy and Future Directions for Sustainable Cloud Computing. ACM Computing Surveys, 51(5), 1–33. https://doi.org/10.1145/3241038

Gonzalez, N. M., Goya, W. A., de Fatima Pereira, R., Langona, K., Silva, E. A., Melo de Brito Carvalho, T. C., Miers, C. C., Mangs, J.-E., & Sefidcon, A. (2016). Fog computing: Data analytics and cloud distributed processing on the network edges. 2016 35th International Conference of the Chilean Computer Science Society (SCCC), 1–9. https://doi.org/10.1109/SCCC.2016.7836028

Hossain, M., Kayas, G., Hasan, R., Skjellum, A., Noor, S., & Islam, S. M. R. (2024). A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. Future Internet, 16(2), 40. https://doi.org/10.3390/fi16020040

Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. Journal of Network and Computer Applications, 98, 27–42. https://doi.org/10.1016/j.jnca.2017.09.002

Ishaq, M., Afzal, M. H., Tahir, S., & Ullah, K. (2021). A Compact Study of Recent Trends of Challenges and Opportunities in Integrating Internet of Things (IoT) and Cloud Computing. 2021 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), 1–4. https://doi.org/10.1109/ICECube53880.2021.9628191

Kamgueu, P. O., Nataf, E., & Ndie, T. D. (2018). Survey on RPL enhancements: A focus on topology, security and mobility. Computer Communications, 120, 10–21. https://doi.org/10.1016/j.comcom.2018.02.011

Kaur, C. (2020). The Cloud Computing and Internet of Things (IoT). International Journal of Scientific Research in Science, Engineering and Technology, 19–22. https://doi.org/10.32628/IJSRSET196657

Kutzias, D., Falkner, J., & Kett, H. (2019). On the Complexity of Cloud and IoT Integration: Architectures, Challenges and Solution Approaches. Proceedings of the 4th International Conference on Internet of Things, Big Data and Security, 376–384. https://doi.org/10.5220/0007750403760384

Lata, M., & Kumar, V. (2021). Standards and Regulatory Compliances for IoT Security. International Journal of Service Science, Management, Engineering, and Technology, 12(5), 133–147. https://doi.org/10.4018/IJSSMET.2021090109

Lee, J. Y., & Lee, J. (2021). Current Research Trends in IoT Security: A Systematic Mapping Study. Mobile Information Systems, 2021, 1–25. https://doi.org/10.1155/2021/8847099

Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., Liang, W., & Xiong, N. (2023). Post-Quantum Security: Opportunities and Challenges. Sensors, 23(21), 8744. https://doi.org/10.3390/s23218744

Malge, S., & Singh, P. (2019). Internet of Things IoT: Security Perspective. International Journal of Trend in Scientific Research and Development, Volume-3(Issue-4), 1041–1043. https://doi.org/10.31142/ijtsrd24010

Mallisetty, S. B., Tripuramallu, G. A., Kamada, K., Devineni, P., Kavitha, S., & Krishna, A. V. P. (2023). A Review on Cloud Security and Its Challenges. 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), 798–804. https://doi.org/10.1109/IDCIoT56793.2023.10053520

Mass, J., Srirama, S. N., & Chang, C. (2020). STEP-ONE: Simulated testbed for Edge-Fog processes based on the Opportunistic Network Environment simulator. Journal of Systems and Software, 166, 110587. https://doi.org/10.1016/j.jss.2020.110587

Mejía-Granda, C. M., Fernández-Alemán, J. L., Carrillo-de-Gea, J. M., & García-Berná, J. A. (2024). Security vulnerabilities in healthcare: an analysis of medical devices and software. Medical & Biological Engineering & Computing, 62(1), 257–273. https://doi.org/10.1007/s11517-023-02912-0

Mohammed Sadeeq, M., Abdulkareem, N. M., Zeebaree, S. R. M., Mikaeel Ahmed, D., Saifullah Sami, A., & Zebari, R. R. (2021). IoT and Cloud Computing Issues, Challenges and Opportunities: A Review. Qubahan Academic Journal, 1(2), 1–7. https://doi.org/10.48161/qaj.v1n2a36

Mota, A. V., Azam, S., Shanmugam, B., Yeo, K. C., & Kannoorpatti, K. (2017). Comparative analysis of different techniques of encryption for secured data transmission. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 231–237. https://doi.org/10.1109/ICPCSI.2017.8392158

Nam, J., Jun, Y., & Choi, M. (2022). High Performance IoT Cloud Computing Framework Using Pub/Sub Techniques. Applied Sciences, 12(21), 11009. https://doi.org/10.3390/app122111009

Nandy, T., Idris, M. Y. I. Bin, Md Noor, R., Mat Kiah, L., Lun, L. S., Annuar Juma'at, N. B., Ahmedy, I., Abdul Ghani, N., & Bhattacharyya, S. (2019). Review on Security of Internet of Things Authentication Mechanism. IEEE Access, 7, 151054–151089. https://doi.org/10.1109/ACCESS.2019.2947723

Nazari Jahantigh, M., Masoud Rahmani, A., Jafari Navimirour, N., & Rezaee, A. (2020). Integration of Internet of Things and cloud computing: a systematic survey. IET Communications, 14(2), 165–176. https://doi.org/10.1049/iet-com.2019.0537

Park, J., & Park, J. (2017). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry, 9(8), 164. https://doi.org/10.3390/sym9080164

Patil, P., Narayankar, P., Narayan D.G., & Meena S.M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science, 78, 617–624. https://doi.org/10.1016/j.procs.2016.02.108

Poonia, V., & Yadav, N. S. (2015). Analysis of modified Blowfish algorithm in different cases with various parameters. 2015 International Conference on Advanced Computing and Communication Systems, 1–5. https://doi.org/10.1109/ICACCS.2015.7324114

Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. Sustainability, 14(18), 11213. https://doi.org/10.3390/su141811213

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. Healthcare, 8(2), 133. https://doi.org/10.3390/healthcare8020133

Shaukat, K., Alam, T. M., Hameed, I. A., Khan, W. A., Abbas, N., & Luo, S. (2021). A Review on Security Challenges in Internet of Things (IoT). 2021 26th International Conference on Automation and Computing (ICAC), 1–6. https://doi.org/10.23919/ICAC50006.2021.9594183

Shukur, H., Zeebaree, S., Zebari, R., Zeebaree, D., Ahmed, O., & Salih, A. (2020). Cloud Computing Virtualization of Resources Allocation for Distributed Systems. Journal of Applied Science and Technology Trends, 1(2), 98–105. https://doi.org/10.38094/jastt1331

Singh, N., Buyya, R., & Kim, H. (2024). Securing Cloud-Based Internet of Things: Challenges and Mitigations. Sensors, 25(1), 79. https://doi.org/10.3390/s25010079

Singh, S., & Chana, I. (2015). Q-aware: Quality of service based cloud resource provisioning. Computers & Electrical Engineering, 47, 138–160. https://doi.org/10.1016/j.compeleceng.2015.02.003

Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and Cloud Computing. Future Generation Computer Systems, 78, 964–975. https://doi.org/10.1016/j.future.2016.11.031

Suresh, M., & Neema, M. (2016). Hardware Implementation of Blowfish Algorithm for the Secure Data Transmission in Internet of Things. Procedia Technology, 25, 248–255. https://doi.org/10.1016/j.protcy.2016.08.104

Surianarayanan, C., & Chelliah, P. R. (2023). Integration of the Internet of Things and Cloud: Security Challenges and Solutions - A Review. In International Journal of Cloud Applications and Computing (Vol. 13, Issue 1). IGI Global. https://doi.org/10.4018/IJCAC.325624

Sutikno, T., & Thalmann, D. (2022). Insights on the internet of things: past, present, and future directions. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(6), 1399. https://doi.org/10.12928/telkomnika.v20i6.22028

Tan, S. F., & Samsudin, A. (2021). Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey. Sensors, 21(19), 6647. https://doi.org/10.3390/s21196647

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102

Tiwari, A. R., & Pangerkar, A. S. (2024). Securing the Cloud: Overcoming Challenges and Implementing Solutions for Effective Cloud Computing Security. In International Journal for Research in Applied Science & Engineering Technology (IJRASET) (Vol. 12). www.ijraset.com

Tsai, M.-J., Lin, P.-Y., & Lee, M.-E. (2023). Adversarial Attacks on Medical Image Classification. Cancers, 15(17), 4228. https://doi.org/10.3390/cancers15174228

Vijayalakshmi V, V. S. (2019). A New Edge Computing Based Cloud System for IoT Applications. International Journal of Recent Technology and Engineering (IJRTE), 8(2), 4289–4293. https://doi.org/10.35940/ijrte.B2759.078219

Walia, R., & Garg, P. (2022). Performance and Security Issues of Integrating Cloud Computing with IoT (pp. 1–12). https://doi.org/10.1007/978-981-16-8774-7_1

Wazir U, K. F. S. S. (2016). Service Level Agreement in Cloud Computing: A Survey. https://sites.google.com/site/ijcsis/

Zakutynskyi, I., Sibruk, L., & Rabodzei, I. (2023). Performance evaluation of the cloud computing application for IoT-based public transport systems. Eastern-European Journal of Enterprise Technologies, 4(9 (124)), 6–13. https://doi.org/10.15587/1729-4061.2023.285514.

Physics-Informed Neural Networks for Predictive Modeling of Energy Dissipation Pathways in IoT-Integrated Smart Solar Grids. (2025). *Albahit Journal of Applied Sciences*, *4*(1), 182-194. https://doi.org/10.65419/albahit.v4i1.56

Design and Implementation of a Low-Cost Multi-Interface Smart Home Automation System for Libyan Households Using Raspberry Pi. (2026). *Albahit Journal of Applied Sciences*, *5*(2), 64-71. https://doi.org/10.65419/albahit.v5i2.138

Mohamed M. Khaleel, Taha Abuali, & Abdulgader Alsharif. (2025). The Role of IT in Developing Smart Grids for Efficient Energy Distribution. *The Open European Journal of Applied Sciences (OEJAS)*, *1*(1), 65-80. https://easdjournals.com/index.php/oejas/article/view/18

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.