Integrating Cloud Computing and Internet of Things: A Systematic Review of Literature

Mashael Saeed Alshahrani[1], Amal Furaih Altamimi[1], Fatemah Hadram Almareq[1], Atta-ur Rahman[2,*], Jamal Alhiyafi[3], Aghiad Bakry[2], Maqsood Mahmud[4], Mohammed Gollapalli[5]

*Correspondence:

[1] Department of Computer Information Systems, [2] Department Computer Science,
College of Computer Science and Information Technology,
Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
[3] Department of Computer Science, Kettering University, Flint, Michigan 48504, USA
[4] School of Computing, Ulster University, Belfast, Northern Ireland, United Kingdom
[5] Department of Information Technology & Engineering, Sydney Metropolitan Institute of Technology,
Sydney, NSW 2000, Australia

Abstract

This systematic review examines the integration of the Internet of Things (IoT) with Cloud Computing (sometimes coined as Cloud of Things), a convergence driving innovation across industries that also presents unique challenges. The study synthesizes research from 2015-2024, focusing on applications, challenges, and opportunities within this rapidly evolving field. A comprehensive search was conducted across IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar, and ACM Digital Library, using relevant keywords and Boolean operators to identify peer-reviewed articles addressing IoT-cloud integration, edge/fog computing, and related architectures. The review adopts a rigorous methodology, including predefined inclusion/exclusion criteria, a multi-stage study selection process, thematic analysis, and SWOT analysis to evaluate recurring themes and assess the strengths, weaknesses, opportunities, and threats of IoT-cloud integration. Critical literature analysis reveals several key themes: architectural innovations in transportation and mobile applications, persistent security and privacy concerns, the rise of edge and fog computing to reduce latency, the need for scalable big data management, and the importance of standardization for interoperability. Research gaps identified include a lack of empirical validation in large-scale deployments, fragmented security frameworks, the absence of unified edge-cloud orchestration, underexplored advanced analytics, and limited open standards. The future research should prioritize real-world testbeds, comprehensive security solutions, integrated edge-cloud ecosystems, intelligent data analytics, open standards, and energy-aware architectures. Addressing these gaps will unlock the full potential of IoT-cloud integration, enabling smarter automation, predictive maintenance, personalized services, and optimized resource utilization across industries. This review offers valuable insights for researchers, practitioners, and policymakers seeking to harness the transformative power of these converging technologies.

Keywords:

Internet of things, cloud computing, cloud of things, technology integration, applications

1. Introduction

The explosive growth of digital technology has completely transformed how individuals, organizations, and civilizations interact with the outside world. Cloud computing and the Internet of Things (IoT) are two of the most notable impacts of these technologies. Both have dramatically enhanced efficiency and spurred innovation across various industries. However, it is widely recognized that the next generation of smart, data-driven applications and services is made possible by the convergence of cloud computing and the IoT (Sergey et al., 2021) [1].

The term "Internet of Things" (IoT) describes a vast network of physically connected objects- sensors and actuators to smart appliances and industrial machines—that collect, transmit, and sometimes process data over wired or wireless networks. These devices operate with minimal human intervention, enabling real-time monitoring, automation, and enhanced decision-making in smart homes, healthcare systems, manufacturing plants, and urban infrastructure. The proliferation of IoT devices has led to an exponential increase in volume, velocity, and variety of generated data, presenting opportunities and challenges for data management and utilization. (Alam, T.,2021) [2]

On the other hand, cloud computing provides on-demand internet access to a shared pool of reconfigurable computing resources, including servers, storage, databases, networks, software, and analytics. Cloud computing enables businesses and individuals to leverage scalable and adaptable IT resources without the need for significant upfront investment in

Manuscript received May 5, 2025
Manuscript revised May 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.5.23

physical infrastructure, thanks to service models such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). As a result of this paradigm shift, high-performance computers and storage have become more widely available, encouraging innovation and operational flexibility (Yadav et al., 2022) [3]. More and more people believe that to fully leverage both technologies, the Internet of Things (IoT) and cloud computing must be combined. Cloud platforms provide the required processing power and storage capacity to process, analyze, and store the massive amounts of data generated by IoT devices. Advanced analytics, machine learning, and artificial intelligence applications are enabled by this connectivity and can lead to smarter automation, predictive maintenance, personalized services, and efficient resource utilization. Furthermore, by centralizing data management and facilitating remote access to services and insights, cloud-based IoT systems can reduce operational costs, improve scalability, and increase system reliability (Sergey et al., 2021) [1].

However, the convergence of IoT and cloud computing also brings its own set of challenges. Security and privacy issues are critical because sensitive data is transmitted across networks and stored in remote data centers. Maintaining strong authentication, data encryption, and regulatory compliance are ongoing concerns. Furthermore, relying on fast and reliable connectivity can be a hindrance, especially in resource-constrained environments or remote locations. Delays in cloud processing can also impact latency-sensitive applications, which is why complementary models such as edge computing and fog computing are being investigated. (Yadav et al.,2022) [3]

Despite these challenges, integrating IoT and Cloud Computing presents significant innovation and efficiency improvement opportunities across industries. It enables real-time monitoring and predictive maintenance in manufacturing, reducing downtime and costs. In healthcare, it supports remote patient monitoring and advanced diagnostics. In transportation, it enhances traffic management and logistics through data-driven insights. The potential for expanding applications is vast, as is the opportunity for developing new business models and services. (Yadav et al.,2022) [3]

Given this field's growing importance and complexity, a systematic review is necessary to synthesize the current state of research, identify key applications, challenges, and opportunities, and highlight gaps that warrant further investigation. This paper aims to provide a comprehensive and critical overview of studies on integrating IoT with Cloud Computing, offering valuable insights for researchers, practitioners, and policymakers seeking to harness the transformative power of these technologies. (Yadav et al.,2022). [3]

This paper is organized as follows: Section 2 provides background and context of the study. Section 3 describes the technology behind smart grids. Sections 4 provides the application of smart grid in smart cities. Section 5 is about the implications of Integrating smart grids into urban infrastructure. study's feasibility, implications, and practicalities. Section 6 is about the sustainable and environmental impact of smart grids. Section 7 sheds light on further development while section 8 concludes the paper.

2. Methodology

2.1. Study Design

This research adopts a systematic review approach to comprehensively identify, analyze, and synthesize peer-reviewed studies focusing on integrating the Internet of Things (IoT) with Cloud Computing. The review emphasizes applications, challenges, and opportunities arising from this integration.

2.2. Data Sources and Search Strategy

Relevant literature was collected from reputable scientific databases, including:

- IEEE Xplore
- ScienceDirect
- SpringerLink
- Google Scholar
- ACM Digital Library

A combination of keywords and Boolean operators was used to maximize coverage, including:

- IoT and Cloud Computing integration
- IoT Cloud architecture
- Edge computing for IoT
- IoT challenges in the cloud
- Cloud-based IoT applications

Operators such as AND, OR, and NOT were used to refine the search results.

2.3. Inclusion and Exclusion Criteria

Inclusion Criteria

- Studies were published between 2015 and 2024.
- Peer-reviewed articles written in English.
- Research directly addresses the integration of IoT with cloud computing, including related paradigms like edge or fog computing.
- Studies focusing on real-world applications, technical challenges, proposed solutions, or architectural frameworks.

Exclusion Criteria

- Studies focus solely on IoT or cloud computing without discussing their integration.
- Non-peer-reviewed articles (e.g., news articles, blog posts, opinion pieces).
- Publications lacking clear methodology or results sections.

2.4. Study Selection Process

The selection process involved several steps:

- Initial Screening: Titles and abstracts were reviewed to eliminate irrelevant studies.
- Full-Text Review: The full texts of potentially relevant articles were examined to ensure they met the inclusion criteria.
- Data Extraction: Key information, including author, year, objectives, methodology, main findings, and identified challenges or solutions, was extracted from each selected study.

2.5. Data Analysis Tools

- Qualitative Analysis: Thematic analysis was used to identify recurring themes, challenges, and opportunities across the selected studies.
- SWOT Analysis: Strengths, Weaknesses, Opportunities, and Threats related to IoT-Cloud integration were systematically evaluated.
- Comparative Tables: Summary tables were created to compare architecture, security issues, and application domains across studies.
- Thematic Coding: Studies were coded based on major topics like security, scalability, latency, and application scenarios.

2.6. Quality Assessment

To ensure the reliability of the review, each study was evaluated according to:

- Clarity of objectives and research questions.
- The soundness of methodology.
- Relevance and recency of references.
- Depth of analysis and discussion.
- Practical significance and applicability of results.

3. Review of Literature

Ashokkumar et al. (2015) [4] conducted a study to develop a multi-layered cloud platform for managing data in intelligent transport systems, leveraging cloud computing and IoT technologies to address growing transportation challenges. The research introduced a unique software framework that integrates vehicle and road infrastructure data into a unified cloud environment to improve driving safety and user experience. The study's strengths lie in its innovative architectural design, its focus on safety, and the effective integration of IoT and cloud platforms. However, it lacks practical evaluation and field trials and does not sufficiently address privacy and security issues. The study opens opportunities for expanding the application of this model to other sectors, such as smart cities, but faces threats from cybersecurity risks and the complexity of integrating heterogeneous devices. Overall, this work represents an important step toward cloud-based intelligent transport systems, but it requires further experimental validation and a stronger focus on security [4].

Atlam et al. (2017) [5] comprehensively reviewed the benefits and challenges of integrating cloud computing with the Internet of Things, proposing a new software architecture enabling billions of devices to connect and exchange data seamlessly. The study is notable for its thorough analysis of technical challenges and opportunities and for presenting a practical architectural model for smart transportation applications. Nevertheless, it lacks real-world experimental validation, mainly focuses on technical aspects without adequately addressing social or economic factors, and only superficially discusses privacy concerns. The study creates opportunities for the development of standardized, scalable platforms and their application in smart cities, but it also faces threats from interoperability and security issues, as well as dependence on stable infrastructure. This

review is valuable for understanding the integration of IoT and cloud computing but would benefit from more practical support and deeper analysis of privacy and security [5].

Dinh et al. (2017) [6] compared a periodic sensing model with a location-based interactive model for providing on-demand sensing services in mobile cloud computing applications. The interactive model focuses on energy efficiency by activating sensors only when needed, based on user location and interests, thus reducing unnecessary data transmission. The study's strengths include improved energy efficiency and spatial interaction, with strong potential for application in smart transportation services. However, it lacks practical validation and presents complexity in device management while not sufficiently addressing security and privacy concerns. The model offers opportunities for use in smart cities and healthcare but faces privacy, connectivity, and scalability threats. The study introduces an innovative approach but requires further field testing and enhanced security measures [6].

Stergiou and Psannis (2017) [7] focused on integrating big data and cloud computing technologies, emphasizing improving security and privacy. The study introduced a new algorithm to enhance big data privacy in cloud environments, particularly within the wireless telecommunications sector. The study's strengths include its focus on security and integrating two core technologies, reflecting a forward-thinking approach. However, it lacks broad field validation and is limited to technical aspects without addressing regulatory or interoperability challenges. The study opens opportunities for applying these solutions in sensitive sectors such as healthcare and finance but faces threats from sophisticated cyberattacks and compliance issues. This work enhances big data security in the cloud but requires more extensive practical development and real-world validation [7].

Yu et al. (2018) [8] reviewed edge computing as a solution for reducing latency and alleviating the load on cloud data centers in IoT applications, categorizing edge computing architectures and comparing their performance in latency, energy consumption, and bandwidth usage. The study's strengths are its comprehensive architectural analysis and quantitative performance comparisons, highlighting the benefits of edge computing for real-time responsiveness. However, it lacks practical case studies and does not sufficiently address security challenges or the complexities of integrating edge and cloud systems. The study points to opportunities for real-time applications and the expansion of edge computing but faces threats from security risks and management complexity. It is an important reference for understanding edge computing in IoT but would benefit from deeper practical exploration [8].

Pourqasem (2018) [9] examined cloud-based IoT platforms' capabilities in processing, communication, and storage, explaining how the cloud can handle, analyze, and store data generated by diverse devices. The study highlighted technical constraints that hinder IoT application development, such as performance and interoperability, and argued that cloud computing offers promising solutions to overcome these challenges. The study's strengths are its comprehensive analysis of technical limitations and its emphasis on the role of the cloud with practical applicability. However, it lacks experimental evaluation, overlooks economic and social aspects, and superficially addresses security and privacy. The study presents opportunities for developing standardized platforms and fostering innovation but faces threats from security risks, interoperability issues, and reliance on infrastructure. This work provides a broad vision of the cloud's role in supporting IoT but requires empirical support and deeper security considerations.

Stergiou et al. (2018) [10] presents an overview of the convergence between cloud computing and the Internet of Things (IoT), focusing on security concerns arising from their integration. The authors highlight mobile cloud computing as an emerging paradigm where data processing and storage are performed outside the mobile device, thus enhancing device efficiency but introducing new security challenges. The study emphasizes that IoT, especially in wireless telecommunications, rapidly expands and enables objects to cooperate over wireless networks to achieve collective goals. The rapid development of both IoT and cloud computing, while promising, also multiplies the attack surface and complexity of securing data and communications. The strength of this work lies in its clear articulation of why robust security frameworks are essential for the future of IoT-cloud systems. However, the study remains largely conceptual, lacking in-depth technical solutions or empirical validation. The opportunity exists to develop new, standardized security architectures tailored to the unique challenges of IoT-

cloud integration. Yet, the fast pace of technological advancement and the ever-evolving nature of cyber threats remain persistent risks that could outpace current security solutions [10].

Shahinzadeh et al. (2019) [11] explore the application of IoT technologies within smart grid infrastructures, focusing on how advancements in embedded systems and ICT have enabled seamless interconnection among various grid components. The study describes how IoT-based technologies, such as advanced controllers, sensors, and meters, facilitate real-time data exchange and management in high-tech environments, including smart buildings and vehicles. The authors clarify that the term internet in this context extends beyond the World Wide Web, encompassing diverse networking architectures. The study's strength is its comprehensive architectural perspective, which underscores IoT's versatility and transformative potential in modernizing energy grids. However, theoretical research lacks empirical demonstrations or real-world deployment results. There is a significant opportunity to develop interoperable IoT solutions that can enhance the intelligence and efficiency of smart grids, but challenges remain regarding integration with legacy systems, security, and regulatory compliance, all of which could hinder large-scale adoption [11].

Yangui (2020) [12] critically evaluates Industrial IoT (IIoT) Platform-as-a-Service (PaaS) architectures, focusing on their suitability for provisioning IIoT applications in cloud environments. The study deliberately excludes generic IoT solutions, instead concentrating on architectures that meet the rigorous requirements of industrial use cases. A set of precise architectural criteria is used for evaluation, and the paper discusses future research directions and persistent challenges. The findings highlight the importance of robust IIoT PaaS platforms for enabling industrial IoT application development, deployment, and management. The strength of this study is its focused, criteria-based assessment of IIoT PaaS architectures, which provides valuable insights for industry stakeholders. However, the evaluation is literature-based and lacks empirical testing or benchmarking of the platforms. The opportunity lies in developing standardized, scalable IoT platforms that foster innovation and interoperability. Nonetheless, the lack of universal standards and the proprietary nature of many solutions present ongoing barriers to widespread adoption [12].

Hamdan et al. (2020) [13] provides a comprehensive survey of edge computing architectures (ECAs) for IoT, outlining the limitations of current approaches and potential solutions. The study discusses how the proliferation of IoT devices and the resulting surge in data generation have exposed the limitations of device resources, making traditional cloud computing insufficient for latency-sensitive applications. Edge-cloud computing, which processes and stores data closer to the source, is presented as a promising solution. The authors categorize ECAs based on criteria such as big data, security, orchestration, and data placement and map them to established IoT layered models. The strength of this work is its thorough categorization and comparative analysis, which serves as a valuable reference for researchers and practitioners. However, the study is mainly descriptive and does not include experimental validation or performance benchmarking. There is an opportunity to develop unified, secure, and efficient edge-cloud frameworks to address latency, scalability, and resource management. Yet, the rapid evolution of edge and IoT technologies and ongoing security and privacy concerns remain significant threats [13].

Stergiou et al. (2021) [14] proposes an innovative, secure infrastructure for managing big data in smart buildings, leveraging the capabilities of a 6G wireless network. The study recognizes that the explosive growth of telecommunications, coupled with the advent of 6G, creates new opportunities for integrating IoT, cloud computing, and edge computing. The core contribution is a secure cache decision system designed to operate in the fog layer of a smart building, enabling safe and efficient internet browsing, data sharing, and big data management. Integrating IoT, cloud, edge, and big data technologies is essential for creating intelligent, secure environments in next-generation wireless networks. The strength of this work is its forward-looking approach, addressing the intersection of multiple emerging technologies with a strong focus on security. However, the research is primarily conceptual and lacks implementation, scalability, and real-world testing details. The opportunity exists to extend this framework to other domains, such as healthcare and transportation, but the immaturity of 6G standards and the complexity of integrating diverse technologies pose significant challenges [14].

Sergi et al. (2021) [1] presents a practical, smart, and secure logistics solution using IoT and

cloud technologies, specifically leveraging the Azure Sphere platform and the MT3620 microcontroller. The study addresses the critical need for real-time monitoring and traceability of perishable goods during transit, a major concern in the logistics industry. The proposed system enables rapid prototyping and deployment, allowing for remote, real-time monitoring of goods' conditions throughout the cold chain. The research highlights the importance of end-to-end security, noting that while rapid prototyping platforms are valuable, ensuring comprehensive security at all levels remains challenging. The strength of this study is its real-world applicability and focus on security and rapid development. However, reliance on specific hardware and proprietary platforms may limit flexibility and broader adoption. There is an opportunity to apply this approach to other sectors, such as pharmaceuticals and supply chain management, but any security vulnerability at any layer could compromise the entire system [1].

Laroui et al. (2021) [15] conducted a comprehensive survey analyzing the roles of edge and fog computing within the Internet of Things (IoT) ecosystem. The study highlights how IoT enables seamless, autonomous communication between devices and digital assets, generating massive volumes of data that must be processed swiftly to maintain application performance and quality of service. The authors argue that traditional cloud computing models are insufficient for real-time IoT requirements, as latency and centralized processing can hinder responsiveness and network efficiency. To address these limitations, the study reviews the emergence of edge and fog computing, which decentralizes data processing by moving computation closer to the data source. This architectural shift enables faster responses, improved resource utilization, and better energy efficiency for latency-sensitive IoT applications. The survey synthesizes current research trends, identifies key challenges such as orchestration, interoperability, and security, and suggests future research directions focused on unified frameworks and scalable, adaptive architectures. The strength of this work lies in its holistic perspective and clear identification of research gaps. However, it remains largely a literature review and would benefit from empirical validation or case studies demonstrating the practical impact of edge and fog computing in real-world IoT deployments [15].

Alam (2021) [2] investigates the pivotal role of cloud-based IoT applications in developing and operating smart cities. The study defines a smart city as an urban area that leverages a network of physical and digital devices to collect data for optimizing city management and services. Cloud-based IoT solutions are instrumental in aggregating and analyzing data from diverse sources such as citizens, devices, homes, and infrastructure to enhance resource management, revenue collection, transportation, utilities, waste management, security, healthcare, and more. The study emphasizes the cloud's role in enabling third-party integration, real-time updates, and scalable data processing, which are essential for smart cities' dynamic and complex environments. Alam's work is notable for mapping out the broad application landscape and demonstrating the transformative potential of IoT-cloud integration in urban contexts. However, the study is primarily descriptive and does not provide an in-depth analysis of technical challenges such as data privacy, interoperability, or latency. Further research could focus on empirical assessments of cloud-based IoT platforms in live smart city environments, focusing on security and citizen trust [2].

Singh et al. (2021) [16] explore the integration of IoT and cloud computing in the context of the COVID-19 pandemic [17-20], emphasizing their critical role in supporting overwhelmed healthcare systems. The study highlights how IoT and cloud technologies facilitate the collection, analysis, and remote monitoring of patient data from various sources, including medical devices, hospitals, ambulances, and senior care facilities. This integration enables rapid decision-making, efficient resource allocation, and reduced direct contact between healthcare professionals and patients, mitigating infection risks. The authors argue that cloud-enabled IoT solutions are crucial for building smart healthcare environments capable of real-time patient monitoring, emergency response, and predictive analytics. The study's strength is its timely focus on a pressing global issue and its illustration of the practical benefits of IoT-cloud integration in healthcare. However, it lacks a detailed discussion of implementation barriers such as data security, interoperability, and the digital divide. Future research should address these challenges and provide case studies or pilot projects demonstrating scalable, secure IoT-cloud healthcare solutions [16].

Wu et al. (2022) [21] proposes a lightweight authentication protocol tailored for IoT-enabled cloud computing environments, addressing the critical need for secure and efficient user authentication in open, heterogeneous wireless networks. As IoT devices proliferate, the risk of security and privacy breaches increases, especially when sensitive data is transmitted over cloud platforms. The study introduces a simple yet robust authentication system, validated through formal security analysis using both the real-or-random model and the ProVerif automatic verification tool and informal analysis. The results demonstrate that the protocol safeguards user privacy and resists common security threats. The main strength of this research is its rigorous security validation and its practical focus on lightweight solutions suitable for resource-constrained IoT devices. However, the study is limited to protocol design and simulation, lacking real-world deployment or performance benchmarking in diverse IoT-cloud scenarios. Further work should explore scalability, interoperability with existing standards, and empirical testing in operational environments [21]. Ramachandra et al. (2022) [22] address the challenges of big data security and privacy in cloud environments by proposing the Triple Data Encryption Standard (TDES) algorithm. The study notes that as big data analytics become increasingly central to various industries, ensuring the confidentiality and integrity of sensitive data stored in the cloud is paramount. Traditional privacy-preserving techniques rely heavily on third parties and may suffer from inefficiencies or inadequate protection. The authors demonstrate that TDES, by increasing key length and complexity, offers a more effective and efficient means of securing large datasets, particularly in healthcare contexts. Experimental results show that TDES outperforms the Intelligent Framework for Healthcare Data Security (IFHDS) regarding faster encryption and decryption times while maintaining strong privacy guarantees. The strength of this study lies in its empirical evaluation and clear comparison with existing methods. However, the research is limited to the healthcare domain and does not address potential scalability issues or integration with other security frameworks. Future studies should investigate the applicability of TDES in other big data contexts and explore hybrid approaches that combine encryption with access control and anomaly detection mechanisms [22].

Almurisi and Tadisetty (2022) [23] investigate the integration of virtualization and cloud computing techniques to address the limitations of traditional Wireless Sensor Networks (WSNs) in supporting IoT applications. The study highlights that as electronic devices and sensing systems become more capable, IoT applications increasingly require dynamic resource sharing, parallel processing, and rapid data acquisition demands that traditional WSNs, with their limited computing power and lack of resource sharing, cannot meet. The authors argue that virtualization enables resource pooling and sharing among multiple applications, while cloud computing provides scalable storage and computational power. By merging IoT-WSN with a cloud-based virtualization environment, the inherent constraints of traditional sensor networks can be overcome, paving the way for more flexible and innovative IoT applications. The study's strength lies in its comprehensive analysis of how virtualization and cloud integration can transform WSN-based IoT systems. However, the research is conceptual and lacks empirical validation or detailed case studies. Future work should focus on real-world deployments, performance benchmarking, and addressing security and interoperability challenges in such integrated environments [23].

Nadeem and Mansour (2022) [24] focus on creating a secure, integrated cloud-based IoT system, particularly for Wireless Sensor Networks (WSNs), by employing a hybrid encryption mechanism that combines the strengths of symmetric and asymmetric algorithms. The study acknowledges that WSNs are foundational to many IoT applications but are hampered by limited resources, especially storage and processing. Cloud computing is presented as a solution to these limitations, enabling efficient data storage and enhanced service delivery. Integrating IoT and cloud computing aims to elevate service efficiency, but the authors identify two major barriers: security and the complexity of large-scale adoption. Their hybrid encryption approach ensures end-to-end security from system analysis and design to implementation, facilitating secure communication between IoT devices and the cloud. The study's strength is its practical focus on security throughout the IoT-cloud lifecycle. However, it lacks extensive empirical results or real-world performance analysis. Further research should evaluate the proposed security mechanisms' scalability, interoperability, and real-world effectiveness.

Kong et al. (2022) [25] provides an extensive survey of edge computing as a paradigm for addressing the limitations of cloud-based IoT architectures. The study notes that the explosive growth of IoT devices has led to massive data generation, which creates bottlenecks such as high network latency and excessive workload on cloud resources when processed centrally in the cloud. Edge computing is a promising solution, shifting data processing closer to the data source and enabling low-latency, scalable IoT systems. The authors observe that while there is a growing body of research on edge computing and IoT, comprehensive studies on their intersection are still scarce. Their survey identifies key challenges, including resource management, security, data consistency, and the need for unified frameworks seamlessly integrating edge and cloud resources. The strength of this work is its broad perspective on current research trends and its identification of research gaps. However, the survey is primarily descriptive and would benefit from more in-depth comparative analysis and case studies demonstrating the practical impact of edge-driven IoT systems [25].

Ansari et al. (2022) [26] conduct a thorough comparative analysis of leading IoT cloud integration platforms, examining their features, capabilities, and challenges associated with their convergence. The study underscores the growing importance of IoT for connecting vast numbers of devices and the critical role of cloud integration in managing this complexity. Using the PRISMA methodology for systematic review, the authors identify and analyze relevant literature, applying bibliometric network analysis to map research trends. They also provide a taxonomy of IoT-based cloud applications and conduct a quality of service (quality of service) factor-based analysis for different domains. The study's strengths are its systematic approach, comprehensive literature coverage, and multi-dimensional analysis of both technological and service-oriented aspects. However, it is primarily literature-based and lacks empirical validation or real-world benchmarking of the platforms discussed. Future research should focus on developing open standards, improving interoperability, and conducting large-scale empirical studies to validate the effectiveness of different IoT-cloud integration approaches.

Verma and Taqa (2022) [27] explore the growing integration of cloud computing and the Internet of Things (IoT) across a wide range of industries. Their study highlights how IoT devices serve as data sources, collecting and transmitting information that is then processed and analyzed in the cloud to deliver real-time insights. By leveraging cloud-based applications, organizations can implement closed-loop systems that respond instantly to data generated by IoT sensors, enabling advanced use cases such as predictive maintenance and analytics. The authors emphasize that cloud computing provides a secure, scalable, and cost-effective environment for managing large-scale IoT deployments, reducing the burden of hardware and software management. This integration not only enhances operational efficiency and control but also makes IoT infrastructure more accessible and affordable for businesses of all sizes. The study's strength lies in its clear articulation of the practical benefits of IoT-cloud convergence, such as improved predictive analytics and streamlined device management. However, the discussion remains largely conceptual, with limited attention to implementation challenges such as data privacy, latency, and interoperability. Future research should focus on empirical validation and address the technical complexities of deploying integrated IoT-cloud solutions on a scale [27].

Yadav et al. (2022) [3] comprehensively survey cybersecurity issues in IoT-based cloud computing environments. The study underscores the transformative impact of cloud computing on data storage, resource sharing, and industrial applications, noting that businesses have rapidly adopted cloud solutions for their performance, cost benefits, and accessibility. However, this swift migration to the cloud has introduced many new security challenges, particularly as conventional security measures often prove inadequate for cloud-based systems. The authors highlight how the proliferation of IoT devices, combined with the adaptable and distributed nature of cloud architectures, has expanded the attack surface and increased vulnerability to cyber threats. The study reviews recent advancements in artificial intelligence and deep learning, which offer promising tools for enhancing cloud security, especially in industrial settings. The strength of this work is its thorough analysis of the evolving threat landscape and the potential of AI-driven solutions. Nonetheless, the survey is primarily descriptive and would benefit from empirical studies or case examples demonstrating the effectiveness of proposed security measures in real-world IoT-cloud deployments. Further research

should address the implementation of advanced security frameworks and the challenges of maintaining privacy and trust in large-scale, heterogeneous environments [3].

Oladimeji et al. (2023) [28] provides an extensive overview of smart transportation technologies and applications, with a particular focus on the role of IoT. The study explains how IoT connects many smart devices, enabling seamless data exchange and communication that underpin modern smart transportation systems. Key benefits include improved traffic management, logistics, parking efficiency, and safety measures in urban environments. The authors also discuss the integration of complementary technologies such as distributed ledgers, big data analytics, and machine learning, which further enhance the capabilities of smart transportation systems through applications like route optimization, accident prevention, and predictive maintenance. The study's strength lies in its holistic perspective on the technological ecosystem supporting smart transportation and its practical examples of real-world applications. However, the review is largely descriptive and does not deeply address challenges such as data security, privacy, or the interoperability of diverse technologies. Future research should focus on empirically evaluating integrated smart transportation solutions, including scalability, user acceptance, and robust security frameworks [28].

Lakhan et al. (2024) [29] introduce the Augmented Federated Learning Lakhan et al. (2024) introduce the Augmented Federated Learning Scheduling Scheme (AFLSS) for efficient workload offloading in intelligent transport systems (ITS) that leverage federated augmented convolutional neural networks (ACNN) across cooperative edge-cloud networks. The study addresses the growing need for real-time, automated decision-making in ITS applications, such as ticket validation, object detection, and collision avoidance. By enabling IoT, especially those with limited resources, to offload computationally intensive tasks to the cooperative edge and cloud nodes, the AFLSS framework improves accuracy and processing speed. The proposed system incorporates various sub-schemes for workload scheduling, security, and collaborative machine learning, allowing efficient and secure operation across distributed networks. Simulation results demonstrate that AFLSS outperforms existing approaches regarding accuracy and total execution time. The main strength of this research is its innovative use of federated learning and edge-cloud cooperation to address real-world ITS challenges. However, the study is based on simulations and would benefit from real-world implementation and testing to assess scalability, interoperability, and robustness under practical conditions. Scheme (AFLSS) for efficient workload offloading in intelligent transport systems (ITS) that leverage federated augmented convolutional neural networks (ACNN) across cooperative edge-cloud networks. The study addresses the growing need for real-time, automated decision-making in ITS applications, such as ticket validation, object detection, and collision avoidance. By enabling IoT, especially those with limited resources, to offload computationally intensive tasks to the cooperative edge and cloud nodes, the AFLSS framework improves accuracy and processing speed. The proposed system incorporates various sub-schemes for workload scheduling, security, and collaborative machine learning, allowing efficient and secure operation across distributed networks. Simulation results demonstrate that AFLSS outperforms existing approaches regarding accuracy and total execution time. The main strength of this research is its innovative use of federated learning and edge-cloud cooperation to address real-world ITS challenges. However, the study is based on simulations and would benefit from real-world implementation and testing to assess scalability, interoperability, and robustness under practical conditions [29].

4. Critical Analysis

Integrating the Internet of Things (IoT) and Cloud Computing is rapidly evolving, driving innovation across manufacturing, healthcare, transportation, and energy. This critical analysis reviews the key studies presented in literature, assesses their contributions and limitations, identifies research gaps, and outlines future research opportunities [30].

4.1. Thematic Synthesis of Literature

4.1.1. Architectural Innovations and Application Domains

Several studies, such as [4-6] have focused on proposing new architectures for IoT-cloud integration, particularly in transportation and mobile applications.

Ashokkumar et al. introduced a multi-layered cloud platform for intelligent transportation systems, emphasizing the need for scalable and secure data management. Likewise, authors in [4] compared periodic sensing models with location-based interactive models to optimize energy efficiency in mobile IoT-cloud applications.

Critical perspective

While these studies contribute valuable architectural frameworks, most are limited to conceptual models or simulations. There is a lack of large-scale, real-world deployments and empirical evaluations. Moreover, the focus is often on a single application domain, such as transportation or mobile computing, without considering cross-domain interoperability or generalizability [31-35].

4.1.2. Security and Privacy Challenges

Security emerges as a predominant concern in IoT-cloud integration, as highlighted by Stergiou and Psannis (2017) [7], Stergiou et al. (2018) [10], and Pourqasem (2018) [9]. These studies discuss privacy issues, propose algorithmic approaches to enhance data confidentiality, and examine the vulnerabilities inherent in cloud-based IoT platforms.

Critical Perspective:

Despite recognizing security as a critical challenge, literature often addresses it in a fragmented manner. Many proposed solutions are theoretical or algorithmic, lacking comprehensive implementation and validation in heterogeneous IoT-cloud environments. There is also insufficient attention to privacy-preserving mechanisms that can operate on a scale, especially in the context of big data and real-time analytics [36-40].

4.1.3. Edge and Fog Computing Paradigms

Yu et al. (2018) [8] and Hamdan et al. (2020) [13] explore the role of edge and fog computing as complementary paradigms to traditional cloud computing. Their surveys highlight how edge computing can reduce latency, distribute computational loads, and improve the responsiveness of IoT applications.

Critical Perspective:

While the shift toward edge and fog computing is well-motivated, the literature reveals a gap in unified frameworks that seamlessly integrate cloud, edge, and fog resources. Existing studies often treat these paradigms in isolation, without addressing orchestration, interoperability, and dynamic resource management across the continuum from edge to cloud [41-45].

4.1.4. Big Data Management and Analytics

Stergiou et al. (2021) [14] and Yangui (2020) [12] address the challenges of managing and analyzing massive volumes of IoT-generated data. They emphasize the need for scalable, secure, and efficient data management architectures, particularly in industrial and smart building contexts.

Critical Perspective:

Although big data analytics is recognized as a key enabler for IoT-cloud integration, current research predominantly focuses on infrastructure and data flow. There is limited exploration of advanced analytics techniques (e.g., machine learning, federated learning) tailored to the unique characteristics of IoT data, such as heterogeneity, sparsity, and real-time requirements [46-50].

4.1.5. Standardization, Interoperability, and Platform Development

Yangui (2020) [12] reviews industrial IoT (IIoT) platform-as-a-service (PaaS) architectures, identifying the need for standardized platforms to support application provisioning and management. Shahinzadeh et al. (2019) [11] discussed IoT architectures for smart grids, highlighting the importance of interoperability among diverse devices and systems.

Critical Perspective:

A major gap in literature is the lack of universally accepted standards for IoT-cloud integration. Most platforms are proprietary or tailored to specific industries, hindering interoperability and scalability. There is also a dearth of open-source

reference implementations and benchmarks for evaluating platform performance [51-55].

4.2. Identified Research Gaps

Based on the critical synthesis above, the following research gaps are evident [56-60]:

- Empirical Validation and Large-Scale Deployment: Most studies are limited to conceptual models, simulations, or small-scale prototypes. Empirical research involving real-world, large-scale deployments is needed to validate proposed architectures and algorithms.
- End-to-end Security and Privacy Frameworks: Security solutions are often fragmented and lack end-to-end coverage. Comprehensive frameworks that address authentication, authorization, data integrity, and privacy across the IoT-cloud continuum are scarce.
- Unified Edge-Cloud-Fog Orchestration: Current research treats edge, fog, and cloud computing as separate silos. Unified orchestration frameworks that enable seamless resource allocation, data migration, and service provisioning across all layers are needed.
- Advanced Data Analytics and Intelligence: The application of advanced analytics, such as distributed machine learning, federated learning, and real-time anomaly detection, is underexplored in IoT-cloud integration.
- Standardization and Interoperability: The lack of standardized protocols, APIs, and data models impedes interoperability. Research on open standards and reference platforms is limited.
- Energy Efficiency and Sustainability: While energy efficiency is mentioned, there is insufficient research on sustainable architecture and green computing practices for IoT-cloud systems.
- Quality of Service (quality of service) and Service Level Agreements (SLAs): Few studies address mechanisms for guaranteeing quality of service and enforcing SLAs in dynamic, heterogeneous IoT-cloud environments.

5. Opportunities for Future Research

To address these gaps, future research should focus on the following directions.

5.1. Real-World Testbeds and Pilot Projects

Develop and deploy large-scale testbeds and pilot projects in diverse sectors (e.g., healthcare, smart cities, transportation) to empirically evaluate the performance, scalability, and security of IoT-cloud integration architectures. Such initiatives will provide valuable insights into practical challenges and user requirements [61-65].

5.2. Comprehensive Security and Privacy Solutions

Design and implement holistic security frameworks that provide end-to-end protection, including lightweight cryptographic protocols, secure data sharing, privacy-preserving analytics, and dynamic threat detection. Emphasis should be placed on usability and scalability in resource-constrained IoT environments [66-70].

5.3. Integrated Edge-Cloud-Fog Ecosystems

Develop unified orchestration platforms that enable dynamic resource allocation, workload balancing, and seamless data migration across edge, fog, and cloud layers. Such platforms should support heterogeneous devices, adaptive networking, and context-aware service provisioning [71-75].

5.4. Intelligent Data Analytics

Advance the application of artificial intelligence and machine learning in IoT-cloud systems, focusing on distributed and federated learning, real-time analytics, and automated decision-making. Research should address the challenges of data heterogeneity, privacy, and limited computational resources at the edge [76-80].

5.5. Open Standards and Interoperability Frameworks

Promote the development and adoption of open standards for data formats, communication protocols, and APIs. Establish reference implementations and benchmarking tools to facilitate

interoperability, portability, and fair comparison of different solutions [81-85].

5.6. Energy-Aware and Sustainable Architectures

Investigate energy-efficient design principles, green computing techniques, and sustainable resource management strategies for IoT-cloud ecosystems. Research should consider the environmental impact of large-scale deployments and explore renewable energy integration [86-90].

5.7. QoS Management and SLA Enforcement

Develop mechanisms for dynamic QoS management and SLA enforcement, leveraging predictive analytics, adaptive resource allocation, and real-time monitoring. Such mechanisms are essential for mission-critical applications with stringent performance requirements [91-95].

5.8. User-Centric and Ethical Considerations

Incorporate user-centric design principles, ethical guidelines, and regulatory compliance into IoT-cloud research. Address issues such as data ownership, consent, transparency, and accountability to foster trust and societal acceptance [96-100].

8. Conclusions and Recommendations

In the current research, the reviewed literature provides a solid foundation for understanding the integration of IoT and Cloud Computing, highlighting significant advancements in architecture, security, edge computing, and data management. However, critical gaps remain, particularly in empirical validation, unified orchestration, standardization, and advanced analytics. Addressing these gaps requires interdisciplinary collaboration, real-world experimentation, and a focus on open, scalable, and secure solutions. Future research should prioritize practical deployment, comprehensive security, intelligent analytics, and sustainable design to unlock the full potential of IoT-cloud integration across industries [101-108].

References

[1] I. Sergi, T. Montanaro, F. L. Benvenuto, and L. Patrono, “A Smart and Secure Logistics System Based on IoT and Cloud Technologies,” Sensors, vol. 21, no. 6, p. 2231, Mar. 2021, doi: 10.3390/s21062231.

[2] T. Alam, “Cloud-Based IoT Applications and Their Roles in Smart Cities,” Smart Cities, vol. 4, no. 3, pp. 1196–1219, Sep. 2021, doi: 10.3390/smartcities4030064.

[3] S. Yadav, K. D. Kalaskar, and P. Dhumane, “A Comprehensive Survey of IoT- Based Cloud Computing Cyber Security,” Oriental journal of computer science and technology, vol. 15, no. 010203, pp. 27–52, Dec. 2022, doi: 10.13005/ojcst15.010203.04.

[4] K. Ashokkumar, B. Sam, R. Arshadprabhu, and Britto, “Cloud Based Intelligent Transport System,” Procedia Comput Sci, vol. 50, pp. 58–63, 2015, doi: 10.1016/j.procs.2015.04.061.

[5] H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills, “Integration of Cloud Computing with Internet of Things: Challenges and Open Issues,” in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, Jun. 2017, pp. 670–675. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105.

[6] T. Dinh, Y. Kim, and H. Lee, “A Location-Based Interactive Model of Internet of Things and Cloud (IoT-Cloud) for Mobile Cloud Computing Applications,” Sensors, vol. 17, no. 3, p. 489, Mar. 2017, doi: 10.3390/s17030489.

[7] C. Stergiou and K. E. Psannis, “Efficient and secure BIG data delivery in Cloud Computing,” *Multimed Tools Appl*, vol. 76, no. 21, pp. 22803–22822, Nov. 2017, doi: 10.1007/s11042-017-4590-4.

[8] W. Yu et al., “A Survey on the Edge Computing for the Internet of Things,” IEEE Access, vol. 6, pp. 6900–6919, 2018, doi: 10.1109/ACCESS.2017.2778504.

[9] J. Pourqasem, “Cloud-Based IoT: Integration Cloud Computing with Internet of Things,” International Journal of Research in Industrial Engineering, vol. 7, no. 4, pp. 482–497, 2018.

[10] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, “Secure integration of IoT and Cloud Computing,” Future Generation Computer Systems, vol. 78, pp. 964–975, Jan. 2018, doi: 10.1016/j.future.2016.11.031.

[11] H. Shahinzadeh, J. Moradi, G. B. Gharehpetian, H. Nafisi, and M. Abedi, “IoT Architecture for Smart Grids,” in 2019 International Conference on Protection and Automation of Power System (IPAPS), IEEE, Jan. 2019, pp. 22–30. doi: 10.1109/IPAPS.2019.8641944.

[12] S. Yangui, “A Panorama of Cloud Platforms for IoT Applications Across Industries,” Sensors, vol. 20, no. 9, p. 2701, May 2020, doi: 10.3390/s20092701.

[13] S. Hamdan, M. Ayyash, and S. Almajali, “Edge-Computing Architectures for Internet of Things Applications: A Survey,” Sensors, vol. 20, no. 22, p. 6441, Nov. 2020, doi: 10.3390/s20226441.

[14] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network," IEEE Internet Things J, vol. 8, no. 7, pp. 5164–5171, Apr. 2021, doi: 10.1109/JIOT.2020.3033131.

[15] M. Laroui, B. Nour, H. Moungla, M. A. Cherif, H. Afifi, and M. Guizani, "Edge and fog computing for IoT: A survey on current research activities & future directions," Comput Commun, vol. 180, pp. 210–231, Dec. 2021, doi: 10.1016/j.comcom.2021.09.003.

[16] N. Singh, M. Raza, V. V. Paranthaman, M. Awais, M. Khalid, and E. Javed, "Internet of Things and cloud computing," in Digital Health, Elsevier, 2021, pp. 151–162. doi: 10.1016/B978-0-12-818914-6.00013-2.

[17] A. Alqarni and A. Rahman, "Arabic Tweets-Based Sentiment Analysis to Investigate the Impact of COVID-19 in KSA: A Deep Learning Approach," Big Data and Cognitive Computing, vol. 7, no. 1, pp. 1-16, 2023.

[18] M. S. Ahmed et al., "Joint Diagnosis of Pneumonia, COVID-19, and Tuberculosis from Chest X-ray Images: A Deep Learning Approach." Diagnostics, vol. 13(1), p. 2562, 2023.

[19] A Rahman, K Sultan, I Naseer, R Majeed, D Musleh et al., "Supervised machine learning-based prediction of COVID-19," Computers, Materials and Continua 69 (1), 21-34, 2021.

[20] R Zagrouba, MA Khan, A Rahman et al., "Modelling and Simulation of COVID-19 Outbreak Prediction Using Supervised Machine Learning," Computers, Materials & Continua 66 (3), 2397-2407, 2021.

[21] T.-Y. Wu, Q. Meng, S. Kumari, and P. Zhang, "Rotating behind Security: A Lightweight Authentication Protocol Based on IoT-Enabled Cloud Computing Environments," Sensors, vol. 22, no. 10, p. 3858, May 2022, doi: 10.3390/s22103858.

[22] M. N. Ramachandra, M. Srinivasa Rao, W. C. Lai, B. D. Parameshachari, J. Ananda Babu, and K. L. Hemalatha, "An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard," Big Data and Cognitive Computing, vol. 6, no. 4, p. 101, Sep. 2022, doi: 10.3390/bdcc6040101.

[23] N. Almurisi and S. Tadisetty, "Cloud-based virtualization environment for IoT-based WSN: solutions, approaches and challenges," J Ambient Intell Humaniz Comput, vol. 13, no. 10, pp. 4681–4703, Oct. 2022, doi: 10.1007/s12652-021-03515-z.

[24] N. Chahin and A. Mansour, "Improvement of the Secure Integration of IoT and Cloud Computing using Hybrid Encryption," International Journal of Electrical Engineering and Computer Science, vol. 4, pp. 66–72, Dec. 2022, doi: 10.37394/232027.2022.4.10.

[25] L. Kong et al., "Edge-computing-driven Internet of Things: A Survey," ACM Comput Surv, vol. 55, no. 8, pp. 1–41, Aug. 2023, doi: 10.1145/3555308.

[26] M. Ansari, S.A. Ali and M. Alam, "Internet of things (IoT) fusion with cloud computing: current research and future direction," International Journal of Advanced Technology and Engineering Exploration, vol. 9, no. 97, Dec. 2022, doi: 10.19101/IJATEE.2021.876002.

[27] D. T. A. R. Verma, "Integrated System: IoT and Cloud Computing," ResearchGate, vol. 9, no. 2, pp. 2394–4331, 2022.

[28] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart Transportation: An Overview of Technologies and Applications," Sensors, vol. 23, no. 8, p. 3880, Apr. 2023, doi: 10.3390/s23083880.

[29] A. Lakhan, T.-M. Grønli, P. Bellavista, S. Memon, M. Alharby, and O. Thinnukool, "IoT workload offloading efficient intelligent transport system in federated ACNN integrated cooperated edge-cloud networks," Journal of Cloud Computing, vol. 13, no. 1, p. 79, Apr. 2024, doi: 10.1186/s13677-024-00640-w.

[30] Alhaidari, F., Rahman, A. & Zagrouba, R. Cloud of Things: architecture, applications and challenges. J Ambient Intell Human Comput 14, 5957–5975 (2023).

[31] N. Aldowesh, A. Alfaleh, M. Alhejazi, H. Baghdadi, A. Rahman, "Electronic Data Interchange Framework for Financial Management System," IJCSNS - International Journal of Computer Science and Network Security 22(6): 275-287, 2022.

[32] W. Hantom, A. Aldweesh, R. Alzaher, A. Rahman, "A Survey on Scheduling Algorithms in Real-Time Systems," IJCSNS, 22(4): 686-690, 2022.

[33] N. AlDossary, S. AlQahtani, H. AlUbaidan, A. Rahman, "A Survey on Resource Allocation Algorithms and Models in Cloud Computing," International Journal of Computer Science and Network Security 22(3): 776-782, 2022.

[34] D Alkhulaifi, M Alqahtani, W Hantom, A Rahman, T Iqbal, "Blockchain Framework for Integrated Petrochemical Complexes," IJCSNS 22 (6), 747-756, 2022.

[35] MAA Khan, O Alsahafi, A Altamimi, Mishary, Alfaleh, N Alsahabi et al., "FutVi: Enhancing Decision Making with Dynamic KPI Insights," IJCSNS - International Journal of Computer Science and Network Security 24(5): 53-64, 2025.

[36] A Al-Qarni, M Al-Shehri, A Rahman, T Iqbal, A Bakry, "Integrating Smart Grids in Smart Cities for Sustainable Future," IJCSNS - International Journal of Computer Science and Network Security 24(5): 227-237, 2025.

[37] A Aslam, J Mir, G Zaman, A Rahman et al., "Extracting Facial Features to Detect Deepfake Videos Using Machine Learning," International Journal of Advanced Computer Science and Applications 16 (4): 834-842, 2025.

[38] M. Zaheer, I.M. Qureshi, A. Rahman, J. Alhiyafi, and M.Z. Muzaffar, "Improved and Secure Differential LSB Embedding Steganography," Journal of Information Assurance and Security 11 (5), 170-178, 2017

[39] M. Al-Dossary, M.S. Alshahrani, A.F. Altamimi, M. Gollapalli, A. Rahman, "Evaluating Mental Health and Well-Being through Social Media Analysis," IJCSNS - International Journal of Computer Science and Network Security, 24 (11):21-34, 2024.

[40] A. Rahman et al., "A neuro-fuzzy approach for user behaviour classification and prediction," Journal of Cloud Computing, vol. 8, no. 1, pp. 1-15, 2019.

[41] G. Zaman, H. Mahdin, K. Hussain, A. Rahman, J. Abawajy and S. A. Mostafa, "An ontological framework for

information extraction from diverse scientific sources," IEEE Access, vol. 9, pp. 42111-42124, 2021.

[42] N.A. Sajid, M. Ahmad, A. Rahman, G. Zaman, M.S. Ahmed, N. Ibrahim et al., "A Novel Metadata Based Multi-Label Document Classification Technique," Computer Systems Science and Engineering 46 (2), 2195-2214, 2023.

[43] S. Arooj, M. F. Khan, T. Shahzad, M. A. Khan, M. U. Nasir et al., "Data fusion architecture empowered with deep learning for breast cancer classification," Computers, Materials & Continua, vol. 77, no.3, pp. 2813–2831, 2023.

[44] F. Jan et al., "Assessing acetabular index angle in infants: a deep learning-based novel approach," J. Imaging, vol. 9, no. 1, p. 242, 2023, doi: 10.3390/jimaging9110242.

[45] M. I. B. Ahmed et al., "Personal protective equipment detection: a deep-learning-based sustainable approach," Sustainability, vol. 15, no. 1, p. 13990, 2023.

[46] M.S. Farooq, S. Abbas, A. Rahman, K. Sultan, M.A. Khan, A. Mosavi, "A Fused Machine Learning Approach for Intrusion Detection System," Computers, Materials & Continua 74 (2), 2607–2623, 2023.

[47] M. I. B. Ahmed et al., "A deep-learning approach to driver drowsiness detection," Safety, vol. 9, no. 65, 2023.

[48] A. Rahman et al., "Geo-Spatial Disease Clustering for Public Health Decision Making," Informatica, vol. 46, no. 6, pp. 21-32, 2022.

[49] M.A. Qureshi et al., "Aspect Level Songs Rating Based Upon Reviews in English." Computers, Materials & Continua 74 (2), 2589-2605, 2023.

[50] T. A. Khan et al., "Secure IoMT for Disease Prediction Empowered with Transfer Learning in Healthcare 5.0, the Concept and Case Study," IEEE Access, vol. 11, pp. 39418-39430, 2023, doi: 10.1109/ACCESS.2023.3266156.

[51] W. H. Hantom and A. Rahman, "Arabic Spam Tweets Classification: A Comprehensive Machine Learning Approach," AI, vol. 5, no. 3, pp. 1049-1065, 2024.

[52] A. Rahman et al., "Rainfall Prediction System Using Machine Learning Fusion for Smart Cities." Sensors, vol. 22, no. 9, p. 3504, 2022, https://doi.org/10.3390/s22093504.

[53] M. Farooqui et al., "A Deep Learning Approach to Industrial Corrosion Detection," CMC-Computers, Materials & Continua, vol. 81, no. 1, pp. 1-19, 2024.

[54] M. N. Alnuaimi et al., "Transfer Learning Empowered Skin Diseases Detection in Children," Computer Modeling in Engineering & Sciences, vol. 141, no. 3, pp. 1-15, 2024.

[55] A. Rahman et al., "Diabetic Retinopathy Detection: A Hybrid Intelligent Approach," Computers, Materials and Continua, vol. 80, no. 3, pp. 4561-4576, 2024.

[56] A. Rehman et al., "Modelling, simulation, and optimization of diabetes type II prediction using deep extreme learning machine," Journal of Ambient Intelligence and Smart Environments, vol. 12, no. 2, pp. 125-138, 2020.

[57] N. M. Ibrahim et al., "Transfer Learning Approach to Seed Taxonomy: A Wild Plant Case Study." Big Data Cogn. Comput., vol. 7, no. 128, 2023.

[58] A. Alhashem et al., "Diabetes Detection and Forecasting using Machine Learning Approaches: Current State-of-the-art," IJCSNS - International Journal of Computer Science and Network Security, vol. 23, no. 10, pp. 199-208, 2023.

[59] M Gul, IA Khan, G Zaman, A Rahman et al., "A Game-Theoretic Approach to Safe Crowd Evacuation in Emergencies," CMC-Computers, Materials & Continua 79 (1), 1631-1657, 2024.

[60] Alabbad, D.A.; Ajibi, S.Y.; Alotaibi, R.B.; Alsqer, N.K.; Alqahtani, R.A.; Felemban, N.M.; Rahman, A.; Aljameel, S.S.; Ahmed, M.I.B.; Youldash, M.M. Birthweight Range Prediction and Classification: A Machine Learning-Based Sustainable Approach. Mach. Learn. Knowl. Extr. 2024, 6, 770-788.

[61] I.A. Qureshi et al., "GFuCWO: A genetic fuzzy logic technique to optimize contention window of IEEE-802.15. 6 WBAN," Ain Shams Engineering Journal, 102681, 2024.

[62] D.M. Althawadi et al., "Exploring Efficient Solutions for the 0/1 Knapsack Problem," IJCSNS, 24(2): 15-24, 2024.

[63] M. M. Qureshi, F. B. Yunus, J. Li, A. Ur-Rahman, T. Mahmood and Y. A. A. Ali, "Future Prospects and Challenges of On-Demand Mobility Management Solutions," in IEEE Access, vol. 11, pp. 114864-114879, 2023.

[64] Musleh DA, Olatunji SO, Almajed AA, Alghamdi AS, Alamoudi BK, Almousa FS, Aleid RA, Alamoudi SK, Jan F, Al-Mofeez KA, et al. Ensemble Learning Based Sustainable Approach to Carbonate Reservoirs Permeability Prediction. Sustainability. 2023; 15(19):14403.

[65] R.A. Qamar, M. Sarfraz, A. Rahman, S.A. Ghauri, "Multi-Criterion Multi-UAV Task Allocation under Dynamic Conditions," Journal of King Saud University-Computer and Information Sciences 35 (9), 101734, 2023.

[66] N. AlDossary, S. AlQahtani, R. Alzaher, A. Rahman, "SYN Flood DoS Detection System Using Time Dependent Finite Automata," International Journal of Computer Science & Network Security 23 (6), 147-154, 2023.

[67] Z. Alsadeq, H. Alubaidan, A. Aldweesh, A. Rahman, T. Iqbal, "A Proposed Model for Supply Chain using Blockchain Framework," IJCSNS - International Journal of Computer Science and Network Security 23(6): 91-98, 2023.

[68] A. Albassam et al., "Integration of Blockchain and Cloud Computing in Telemedicine and Healthcare," IJCSNS, 23 (6): 17-26, 2023.

[69] Sajid, N.A. et al. Single vs. Multi-Label: The Issues, Challenges and Insights of Contemporary Classification Schemes. Appl. Sci. 2023, 13, 6804.

[70] Gollapalli, M. et al. SUNFIT: A Machine Learning-Based Sustainable University Field Training Framework for Higher Education. Sustainability 2023, 15, 8057.

[71] Talha, M.; Sarfraz, M.; Rahman, A.; Ghauri, S.A.; Mohammad, R.M.; Krishnasamy, G.; Alkharraa, M. Voting-Based Deep Convolutional Neural Networks (VB-DCNNs) for M-QAM and M-PSK Signals Classification. Electronics 2023, 12, 1913.

[72] Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. J. Sens. Actuator Netw. 2023, 12, 29.

[73] Alghamdi, A.S.; Rahman, A. Data Mining Approach to Predict Success of Secondary School Students: A Saudi Arabian Case Study. Educ. Sci. 2023, 13, 293.

[74] Rahman, A. GRBF-NN based ambient aware realtime adaptive communication in DVB-S2. J Ambient Intell Human Comput 14, 5929–5939 (2023).

[75] Ahmad, M. et al. Enhanced query processing over semantic cache for cloud based relational databases. J Ambient Intell Human Comput 14, 5853–5871 (2023).

[76] Basheer Ahmed, M.I et al., A Real-Time Computer Vision Based Approach to Detection and Classification of Traffic Incidents. Big Data Cogn. Comput. 2023, 7, 22.

[77] M Jamal, NA Zafar, D Musleh, MA Gollapalli, S Chabani, "Modeling and Verification of Aircraft Takeoff Through Novel Quantum Nets." Computers, Materials & Continua 72 (2), 3331-3348, 2022.

[78] Q. Hussain, A.S.M. Noor, M.M. Qureshi, J. Li, A. Rahman, A. Bakry et al., "Reinforcement learning based route optimization model to enhance energy efficiency in internet of vehicles," Scientific Reports 15, 3113, 2025.

[79] M. Youldash et al., "Early Detection and Classification of Diabetic Retinopathy: A Deep Learning Approach." AI, 5(4), 2586-2617, 2024. https://doi.org/10.3390/ai5040125.

[80] A. Rahman et al., "Histopathologic Oral Cancer Prediction Using Oral Squamous Cell Carcinoma Biopsy Empowered with Transfer Learning." Sensors, 22(10), 3833, 2022.

[81] M. Mahmud, A. Rahman, M. Lee, J.Y. Choi, "Evolutionary-based image encryption using RNA codons truth table," Optics & Laser Technology 121, 105818, 2020.

[82] Ghazal, Taher M et al. "Supervised Machine Learning Empowered Multifactorial Genetic Inheritance Disorder Prediction." Computational intelligence and neuroscience vol. 2022 1051388. 31 May. 2022,

[83] Adnan Khan M, Abbas S, Atta A, Ditta A, Alquhayz H, Farhan Khan M, et al. Intelligent cloud based heart disease prediction system empowered with supervised machine learning. Comput Mater Contin. 2020;65(1):139–151.

[84] S. Dash, S. BISWA, D. BANERJEE, A. Rahman, "Edge and Fog Computing in healthcare – a review," Scalable Computing: Practice and Experience 20 (2), 191-205, 2019.

[85] Rahman, Au., Dash, S. & Luhach, A.K. Dynamic MODCOD and power allocation in DVB-S2: a hybrid intelligent approach. Telecommun Syst 76, 49–61 (2021).

[86] Rahman, A. GRBF-NN based ambient aware realtime adaptive communication in DVB-S2. J Ambient Intell Human Comput 14, 5929–5939 (2023).

[87] Ibrahim, N.M., Gabr, D.G.I., et al. A deep learning approach to intelligent fruit identification and family classification. Multimed Tools Appl 81, 27783–27798 (2022).

[88] F. Alhaidari et al., "Intelligent Software-Defined Network for Cognitive Routing Optimization Using Deep Extreme Learning Machine Approach," Comput. Mater. Contin., vol. 67, no. 1, pp. 1269–1285, 2021.

[89] F. Alhaidari et al., "ZeVigilante: Detecting Zero-Day Malware Using Machine Learning and Sandboxing Analysis Techniques," Computational Intelligence and Neuroscience 2022, 1615528, 15 pages, 2022.

[90] M. Gollapalli et al., "Appendicitis Diagnosis: Ensemble Machine Learning and Explainable Artificial Intelligence-Based Comprehensive Approach." Big Data and Cognitive Computing, 8(9), 108, 2024. Doi: 10.3390/bdcc8090108.

[91] S. Abbas, S.A. Raza, M.A. Khan, A. Rahman, K. Sultan, and A. Mosavi, "Automated File Labeling for Heterogeneous Files Organization Using Machine Learning." Computers, Materials & Continua 74 (2), 3263-3278, 2023.

[92] M. Zaheer, I.M. Qureshi, K. Sultan, A. Rahman, M.Z. Muzaffar, R. Alnanih, "High Capacity Image Steganography Based on Prime Series Representation and Payload Redundancy Removal," Journal of Information Assurance and Security 14 (2), 40-47, 2019.

[93] A. Rahman, S.A. Alrashed, A. Abraham, "User Behaviour Classification and Prediction Using Fuzzy Rule Based System and Linear Regression," Journal of Information Assurance and Security 12 (3), 86-93, 2017.

[94] D.A. Almubayedh et al., "Quantum bit commitment on IBM QX," Quantum Information Processing 19 (55), 2020.

[95] A. Rahman, "Memetic computing based numerical solution to Troesch problem," Journal of Intelligent and Fuzzy Systems 36 (6), 1-10, 2019.

[96] A. Rahman, "Optimum information embedding in digital watermarking," Journal of Intelligent & Fuzzy Systems 37 (1), 553-564, 2019.

[97] H. Yigang, F. Ali, A.A. Cheng Weiding et al., "A Review on Spectrum Standardization for Wireless Networks: Past, Present and Future Advancements," The Intersection of 6G, AI/Machine Learning, and Embedded Systems: Pioneering Intelligent Wireless Technologies, CRC Press, 2025.

[98] B Al-Hamad, N Al-Dossary, H Al-Muhaisen, M Gollapalli, A Rahman et al., "Minimum Data Set (MDS) in Saudi Arabia's Medical Claims Insurance," IJCSNS - International Journal of Computer Science and Network Security, vol. 25, no. 2, pp. 50-60, 2025.

[99] S Bosbait, R Alrayes, M Aldahoos, F Almareq, M Gollapalli et al., "A Retrospective Analysis of Appendicitis Symptoms in Saudi Arabia," IJCSNS, vol. 25, no. 2, pp. 39-49, 2025.

[100] F. Ali, H. Yigang, A. Rahman, C.W. Ding, A. Ali, D. AlKhulaifi et al., "A Novel Reliable Approach to Measure Error Sensitivity in Signal Transmission," International Journal of Intelligent Engineering and Systems 18 (2), 90-100, 2025. Doi: 10.22266/ijies2025.0331.08.

[101] A. Dilawari et al., "Natural Language Description of Videos for Smart Surveillance." Applied Sciences. 2021; 11(9):3730.

[102] M. Gollapalli et al., "A Neuro-Fuzzy Approach to Road Traffic Congestion Prediction," Comput. Mater. Contin., vol. 73, no. 1, pp. 295–310, 2022.

[103] A. Rahman, I.M. Qureshi, N.A. Malik, M.T. Naseem, "A Real Time Adaptive Resource Allocation Scheme for OFDM Systems Using GRBF-Neural Networks and Fuzzy Rule Base System," International Arab Journal of Information Technology 11 (6), 593-601, 2014.

[104] A. Rahman, K. Sultan, N. Aldhafferi, A. Alqahtani, M. Mahmud, "Reversible and Fragile Watermarking for Medical Images," Computational and mathematical methods in medicine, 2018, doi:10.1155/2018/3461382.

[105] K.A. Bhatti, B. Rauf, I.A. Qureshi, A. Majeed, A. Rahman, A. Alqahtani, "Adaptive source transmission rate algorithm for IoT network," Expert Systems with Applications 281, 127254, 2025. https://doi.org/10.1016/j.eswa.2025.127254.

[106] Atta-ur-Rahman, Dash, S., Ahmad, M., Iqbal, T. (2021). Mobile Cloud Computing: A Green Perspective. In: Udgata, S.K., Sethi, S., Srirama, S.N. (eds) Intelligent Systems. Lecture Notes in Networks and Systems, vol 185. Springer, Singapore. https://doi.org/10.1007/978-981-33-6081-5_46.

[107] R Zagrouba, A AlAbdullatif, K AlAjaji, N Al-Serhani, F Alhaidari et al., "Authenblue: A New Authentication Protocol for the Industrial Internet of Things," Computers, Materials & Continua 67 (1), 1103-1119, 2021.

[108] G Zaman, H Mahdin, K Hussain, A Rahman, N Ibrahim, NZM Safar, "Digital Library of Online PDF Sources: An ETL Approach," IJCSNS 20 (11), 172-181, 2020.