Volume 1, 2025, Pages 11-21 *Elaris Computing Nexus*
| Regular Article | Open Access

Edge and Cloud Computing Architectures in IoT A Systematic Review on Applications Security and Resource Management

Prathap Mani
Department of Computer Science and Information Technology, American University of Kurdistan, Sumel, Iraq
prathap.mani@auk.edu.krd

Article Info
Elaris Computing Nexus
https://elarispublications.com/journals/ecn/ecn_home.html

https://doi.org/10. XXXX/ECN/2025002

Received 15 January 2025
Revised from 12 March 2025
Accepted 18 March 2025
Available online 06 April 2025
Published by Elaris Publications.

Corresponding author(s):
Prathap Mani, Department of Computer Science and Information Technology, American University of Kurdistan, Sumel, Iraq
Email: prathap.mani@auk.edu.krd

Abstract – Companies have identified edge-to-cloud integration as a valid way to improve the efficiency of Internet of Things (IoT) systems through the provision of data processing capability and security, and a range of other resource management services. This study entails a literature analysis of the present state of progress in the development of edge and cloud computing architecture with their applications, challenges, and possible solutions. The review reflects the effectiveness of the designs in vital fields like health, safety, privacy, and optimization of resources. It also discusses the methods that are considered hybrids, namely fog computing, and how it may be applied to IoT-related issues of lower latency, energy saving, and offloading. In general, this paper provides an in-depth review of the existing body of knowledge in terms of registration and mapping analysis, identification of trends and novel technologies like federated learning and blockchain.

Keywords – Cloud Computing, Edge Computing, IoT, Hybrid Systems, Fog Computing, Security, Resource Management, Healthcare, Privacy, Task Offloading.

I. INTRODUCTION

Cloud computing is essential in the IoT ecosystem, serving as the computational foundation that facilitates the storing, processing, and analysis of the substantial data produced inside the IoT framework. It transcends the constraints of localized hardware systems and unleashes the transformative potential of AI and IoT. Cloud systems offer a containerized approach to the fluctuating demands of IoT solutions, effectively managing information surges that may occur during public gatherings or natural disasters in smart cities. During periods of diminished activity, resources can be adjusted to sustain cost efficiency, which is essential for green IoT implementation. Besides improving scalability level, integration of AI in cloud has revolutionized the raw data processing capacity to come up with actionable knowledge. Companies use machine learning platforms such as Microsoft Azure AI, Google Vertex AI, and AWG SageMaker are commercial-based machine learning systems to implement machine learning models [1].

Edge computing has become the new solution in the IoT scenario addressing problems of real-time decisions, bandwidth, and latency. This method reduces the overdependence on centralized cloud facilities and processes the data closer to the origin at the edge of the network. Latency matters a lot to other applications such as in autonomous vehicles, remote health, and industrial drives, not just as a bonus. The other important capability within this area is the ability to perform AI inference alongside edge devices. The available frameworks that allow applying AI on low-resource mobile devices are PyTorch Mobile and TensorFlow. This feature allows edge devices to process data locally and thereby removes the requirement of transferring significant amounts of data to distant cloud processes [2].

IoT proliferation brings many concerns specifically privacy and security issues. Sensor nodes are mostly commonly used in autonomous systems, and therefore they need a thorough security control to prevent threats. Privacy, in this context, refers to the right of the individual to control and protect personal data against improper tracking and usage. The idea is synonymous with informational privacy, which regards the management of personal information. It is contrasted with other forms of

privacy including physical privacy which is the declaration of spatial limits of an individual; and decisional privacy which is the ability to make personal decisions and choices free from coercion or interference. Security is in regard to shielding information and hardware against malicious attacks and unlawful alterations. A correlation of privacy and security is crucial in ensuring the reliability and soundness of IoT networks. Privacy preserving security solutions aim at guaranteeing the user privacy and network security, as well as the effective implementation of these solutions.

Healthcare is highly dependent on several sensors, pacemakers and ultrasound scanners for instance, to evaluate a patient's status. The vast quantities of data generated by this technology necessitate substantial computational resources for processing and analysis. To mitigate costs and manage reliance on on-premises technology, several healthcare institutions have transitioned to cloud computing. This change presents new obstacles. Patient data will necessitate transmission to and across cloud servers and may be affected by latency and heightened security protocols. Wearable sensors communicate with mobile EMS units mostly via cellular networks, which may expose critical data to potential hacking threats. To mitigate these concerns, organizations operating in the healthcare sector typically utilize VPNs to direct information through a centralized firewall prior to transmitting it to cloud [3].

This security technique can create a bottleneck that hinders data transfer and impedes real-time analysis, essential for prompt medical treatments. In contrast to central processing, edge computing localizes patient data processing, resulting in significantly reduced processing times. This method utilizes computing resources within the same network as the data source. A clinic may possess edge computers in conjunction with networking equipment, but an ambulance can be equipped with a compact device that consolidates cellular connectivity, routing, and data processing. Certain medical devices provide processing capabilities, enabling near-instantaneous data analysis. Edge computing significantly diminishes latency by processing data closer to its origin, hence enhancing application speed and accuracy. Furthermore, maintaining data within the local network diminishes the probability of interception. Moreover, SD-WAN technology facilitates secure remote monitoring of patient health data without reliance on VPNs, hence enabling rapid responses to critical alerts.

We introduce a systematic review (SR) of edge and cloud computing systems in the area of IoT application and research with the emphasis on their usage in healthcare, security and resource management. We also review hybrid systems like fog computing which have proved to alleviate issues like latency, power consumption, and offloading.

The remaining sections of this review have been organized in the following structure: Section II reviews related work on edge and cloud computing architectures in IoT. Section III describes our research methodology, which integrates literature search, data extraction, keyword analysis, thematic synthesis, and use case evaluation. We present a discussion of the results in Section IV highlighting SR organization, bibliometric assessment, keyword analysis, and application cases. Lastly, Section V concludes the study and highlights the incorporation of cloud and edge computing architectures within the IoT domain.

II. RELATED WORKS

Liu et al. [4] presented an extensive analysis of the IoTs, such as IoT topologies, foundational technologies, and concerns about security and privacy. They also examined the integration of IoT with edge and fog computing about applications. Nevertheless, they did not examine IoT applications. Al-Fuqaha et al. [5] provides an exhaustive analysis of IoT protocols, applications, and technologies. Hui, Sherratt, and Sánchez [6] analyzed IoT applications by consumer category and popularity, classifying them into personal, smart surroundings, houses, and cars. Cvar et al. [7] examined 20 IoT application cases across three primary IoT applications: intelligent households, intelligent cities, and intelligent regions.

Ren et al. [8] presented a model that improves service allotment by using open computing to fully use edge-computing devices, hence enhancing expandability and minimizing response latency. This model comprises multiple layers: the end-user layer, integrating IoT instruments; the end-server layer, tasked with providing services to users; the backbone network, facilitating interaction between the cloud and edge computing machines that encompasses storage resources and robust computing for managing complex and large-scale data; and interface and management layer, tasked with overseeing the whole architecture.

Suciu et al. [9] recommended a system, which improves e-medical applications, comprising the following elements; a manager, which coordinates the other elements; a communications engine, which manages radio interfaces; a device manager, which segregates technology-centric activities from communication-centric services; a device manager, which adaptively loads certain protocols; a database, which stores device statuses; interface control, which facilitates communication between the cloud and E-ALPHA devices; and a GUI that offers access to software configurations modules. The system was modeled via EdgeCloudSim.

Security in healthcare enhances quality while reducing costs. Our approach outlines a structure that ensures security, privacy, and performance within the healthcare system. **Fig. 1** illustrates the Patient and Health Service Provider sharing the key, which comprises both a private and a public key. The patient transmits coded data accompanied by an e-signature to the healthcare service provider. Upon obtaining messages from a patient, the provider decrypts messages and validates signatures. If validated, the provider encrypts the user health data in accordance with the patient's specified policy. Following the transfer of this health data to the healthcare provider, PHI is kept on the cloud system.

Hsu and Lin [10] assert that although the substantial advantages consumers get from the Internet of Things, there are accompanying problems that need examination. The predominant issues identified are cybersecurity and privacy hazards. These two provide a significant dilemma for several corporate and public organizations. Prominent cybersecurity breaches have shown the weaknesses of IoT devices. The interconnection of networks in the IoT necessitates accessibility from

untrusted and anonymous sources, hence demanding innovative security solutions. Conversely, it is crucial to underscore the standards and critical concepts of the IoT cyber security model in the application of the IoT security model.

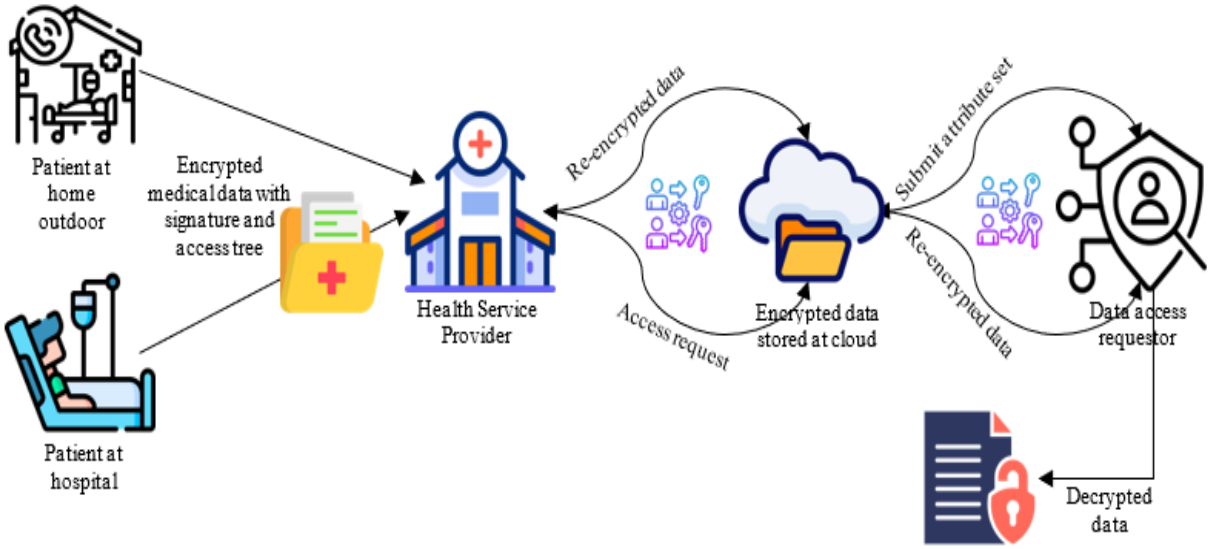

Fig 1. Existing Framework of Health Information Technology Security

As stated by Gerpott, Ahmadi, and Weimar [11], a critical consideration is the termination of a contract involving several instruments with various communications protocols. The difference in protocols obstructs the establishment of various service contracts and integrates fundamental elements, which must be included into the cybersecurity structure of every IoT device. The scholars illustrated that to guarantee the reliability of the IoT model in the cybersecurity domain; incremental measures must be implemented to mitigate the challenges linked to IoT cybersecurity.

Furthermore, Tariq et al. [12] shown that scalability is a critical metric for evaluating the efficacy of the cybersecurity IoT architecture. The scholars argue that the IoT system should possess the adaptability to address a billion cybersecurity- and internet-related concerns. Furthermore, they emphasized that the IoT cybersecurity domain must also enable testability, including system testing, integration testing, compliance testing, and component assessment, therefore effectively mitigating threats.

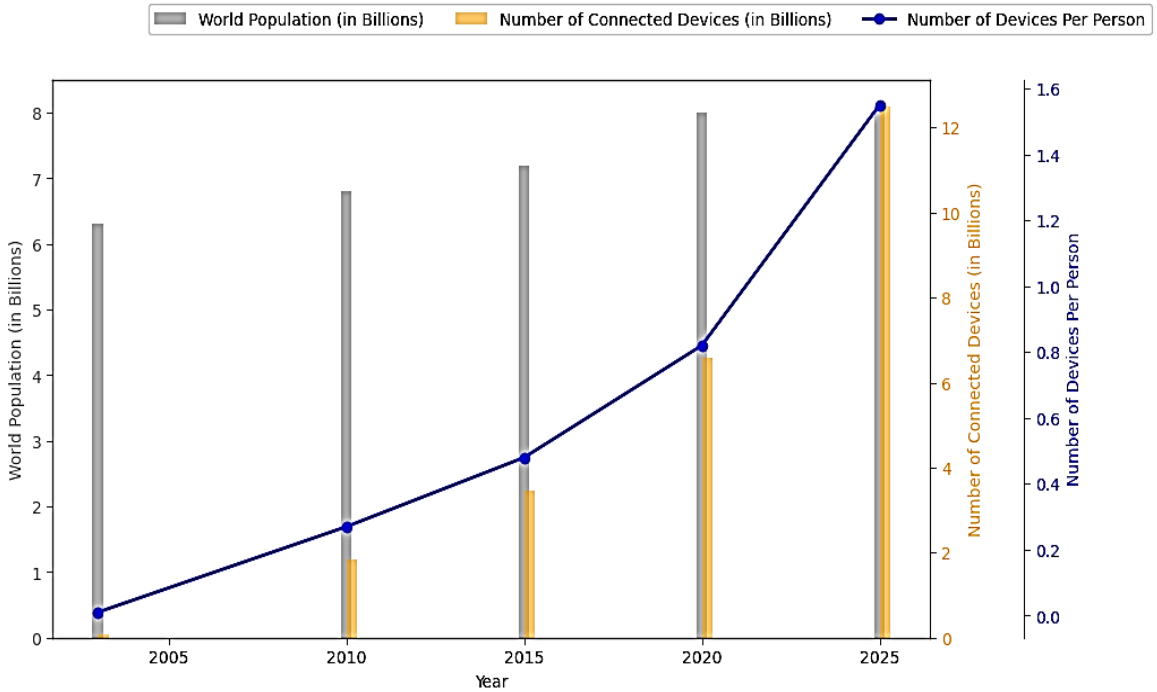

Fig 2. No. of Devices Anticipated to Be Linked to The Internet by 2025

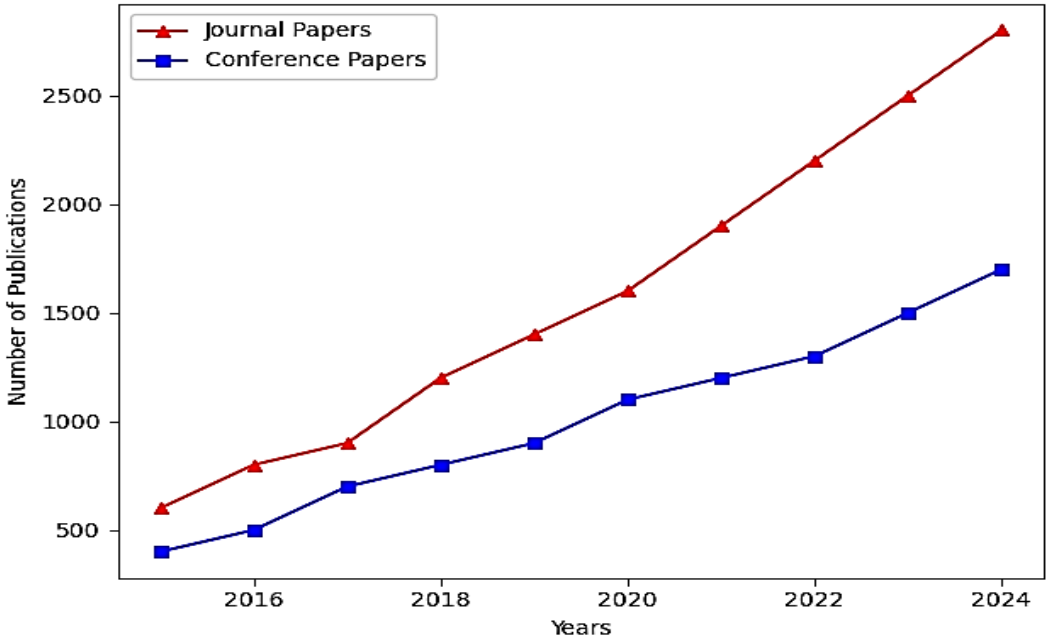

Fig 3. IoT Research Pattern from 2015

The report indicates that the number of IoT device is projected to reach 75.45 billion, and the economic development of IoTs technology is expected to range from $2.71 trillion to $6.22 trillion by 2025; this underscores the influence of IoT on society. **Fig. 2** depicts the anticipated number of IoT devices by 2025, which are projected to create roughly 80 Zettabytes of data. **Fig. 3** illustrates the research advancements in the domain of IoT using IEEE Xplore in the search and selection procedure.

Villegas-Ch et al. [14] provide a hybrid architecture (refer to **Fig. 4**) that integrates the frameworks of Artificial Intelligence and blockchain. This architecture has four intelligence blocks designed to create a system capable of attaining a high degree of security via big data analysis, applicable in smart transit, smart cities, and smart healthcare. Phalaagae et al. [15] provide a unique hybrid model, which amalgamates attenuation methods, gated recurrent units (GRU), bidirectional long short-term memory (BLSTM), and convolutional neural networks (CNN) to enhance the security of IoT. It utilizes the advantages of every method to establish a synergistic model proficient in identifying and categorizing a wide array of cyber-attacks with high accuracy and few false positives. The suggested paradigm is meant to be adaptable, assuring its application across various IoT environments, from resource-based sensors to more advanced devices.

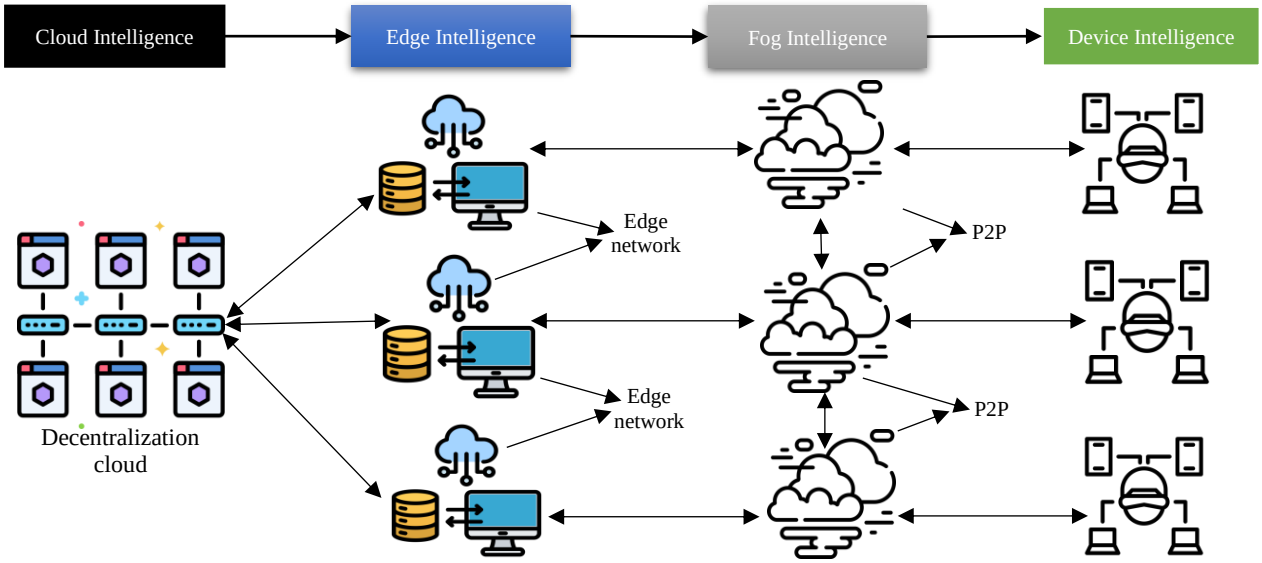

Fig 4. Architecture of the Hybrid System, Adapted from [13]

III. RESEARCH METHODOLOGY

This research will utilize a systematic review (SR) approach to synthesize and analyze current studies on cloud and edge computing as part of the IoT. The main aim will be to discuss the existing state of research, major issues and prospects in the fields, and evaluate the role of these technologies in healthcare, security, privacy, and resources management. This approach provides a clear, reproducible, and multi-faceted examination of the scarce literature, in accordance with the recommendations of SR applied to the sphere of computational studies and IoT systems.

Literature Search and Selection Criteria

The research commenced with a broad survey of scholarly sources in several well-regarded databases, Google Scholar ScienceDirect, SpringerLink, and IEEE Xplore. Search queries were constructed as follows: using terms such as edge computing, cloud computing, IoT, security, privacy, fog computing, and healthcare applications to identify a broad selection of literature works. The search window was limited to those works published between 2018 and 2023 to make the review relevant to the last advances in edge and cloud computing technologies, their applications, and their integration with IoT.

To guarantee the quality and relevance of the selected papers, strict inclusion/exclusion criteria were used. Studies were peer-reviewed, and inclusion criteria were met provided they address edge and cloud computing paradigms within the context of IoT, with specific emphasis on security and privacy, healthcare, resources management, and hybrid systems. Research articles which were not peer-reviewed, written in languages other than English and irrelevant to core topics of the review were excluded. The selection was iterative, where a large pool of studies was selected and finally narrowed down to a set of articles based on their relevance to the research questions and methodological rigor.

Data Extraction and Categorization

The selected studies were read, and data extraction was conducted to provide the information that is already needed. This involved information about publication year, research objectives, methods, results, and area of study covered by the IoT. The collected information was, then, divided into grand thematic chapters: edge and cloud computing structures, safety and privacy, resource utilization, and health (medical) applications.

Table 1 presents these categories, and provides an overview of the themes that were identified in the studies. Different categories were evaluated to identify emerging issues, responses, and research gaps, which would adequately give directions to the thematic synthesis. The categorization process was crucial to the process of organizing the data and making the trend analysis in the literature easily paced.

Table 1. Summary of Themes Across Studies

Research Theme	Key Findings	Ref.
Edge and Cloud Computing	Hybrid architectures like fog computing are gaining traction for balancing latency, privacy, and scalability. Edge computing is preferred for low-latency applications, while cloud offers scalability.	[16]
Security and Privacy	Edge computing enhances privacy by processing data locally. Security challenges include data transfer and endpoint vulnerabilities. Blockchain is explored for secure data exchange.	[17]
Healthcare Applications	Edge computing enables real-time monitoring and data processing in healthcare, while hybrid systems address privacy concerns. Data security remains a key challenge.	[18]
Resource Management	Task offloading and energy efficiency are central to optimizing resource use in IoT systems, with strategies aimed at minimizing latency and maximizing device performance.	[19]
Fog Computing	Fog computing is increasingly used to reduce latency in critical IoT applications like autonomous vehicles and smart cities by combining edge and cloud capabilities.	[20]

Besides category classification, bibliometric analysis of the works was done to determine the period of publication distribution, geographical distribution and areas of interest and focus. The qualitative approach to research helped to define some key trends of the study such as the increasing interest in hybrid computing solutions such as fog computers, the trend of interest growth in healthcare topics over the past few years.

Keyword Analysis and Co-occurrence Network

To better comprehend the relation between the key research concepts, the harvested data was run through a keyword search. This was to be used to determine the most frequently used terminologies in the literature and the relationship thereof. A word

cloud was generated to present a visual distribution of these words, with edge computing, IoT, security, and privacy being the most frequent ones in the studies. Furthermore, a connected network of popular keywords was constructed in order to visualize associations among these words. This map represents interconnections between the research topics such as edge computing, cloud computing, privacy, machine learning, and fog computing. The co-occurrence network provides a visual illustration of how different topics are related, and, it demonstrates how the entire cloud computing study in edge computing is a collaborative work.

Thematic Synthesis

After the categorization and the keyword analysis, the thematic synthesis was carried out with the aim of containing the major trends and challenges covered in the studies. The synthesis has been centered on four key themes.

Edge and Cloud Computing Architectures

The review compared the various architectural paradigm used in IoT systems which include purely edge-based, purely cloud-based, and hybrid or fog computing. It discussed the advantages and disadvantages of one another, especially when it comes to better performance, diversification, latency, and solitude issues. The trade-off between use of edge and cloud computing was at the heart of the analysis because edge computing provides low latencies and added privacy due to local processing of data, whereas cloud computing offers scalability and computing might.

Privacy and Security

This theme centered on security weaknesses of the IoT systems and the precautions that are being suggested in order to protect user data. Some of the essential subjects were data encryption, access control and privacy-preserving methods, e.g., differential privacy and secure computation. The synthesis also explained why authentication and guaranteed communication is vital in curbing risks such as man-in-the-middle attacks.

Resource Management and Optimization

The review considered the resource management approach, including task offloading and energy optimization in edge computing. Most IoT devices are limited to power and computational capabilities therefore an important task is how to manage the workload between the edge nodes and the cloud. Some studies offered the idea of dynamic task offloading algorithms to reduce energy use and maximize resource usage.

Healthcare Applications

The review considered both applicability of edge and cloud computing technologies in healthcare, specifically remote patient monitoring, real-time diagnostics, and AI-based college medical services. Important elements like privacy, data security, and data processing in real-time were addressed thoroughly, with edge computing delivering low data latency processing and cloud computing large data storage capacity and sophisticated analysis.

Use Case Evaluation

To put the findings into practical context, a thorough use case analysis is carried out targeting healthcare as a realistic domain of applications of edge and cloud computing in IoT. The healthcare industry is another field where edge computing is particularly useful owing to the requirement of real-time surveillance and low latency actions. As an example, wearable health devices are able to process data on an edge node, speeding up crucial analysis and reducing the amount of sensitive patient data transmitted back to the cloud. The cloud, meanwhile, remains a vital aspect in storing and analyzing large volumes of data, especially during long-term patient observation and more complex AI-based diagnostics.

IV. RESULTS AND DISCUSSION

SR Organization

Our SR is structured as follows:

- We first examine the pertinent subjects found in the reviewed literature, including safety, security, energy, optimization, and healthcare.
- We then examine the application of data analysis and the preservation of privacy within these frameworks. Subsequently, we evaluate the merits and demerits of edge and cloud computing within the framework of IoT solutions.
- We subsequently explore computing designs, emphasizing hybrid systems that integrate the advantages of both cloud and edge computing. Fog computing exemplifies a significant hybrid system, which we will examine thoroughly.

Fig. 5 provides a summary of the primary subjects examined.

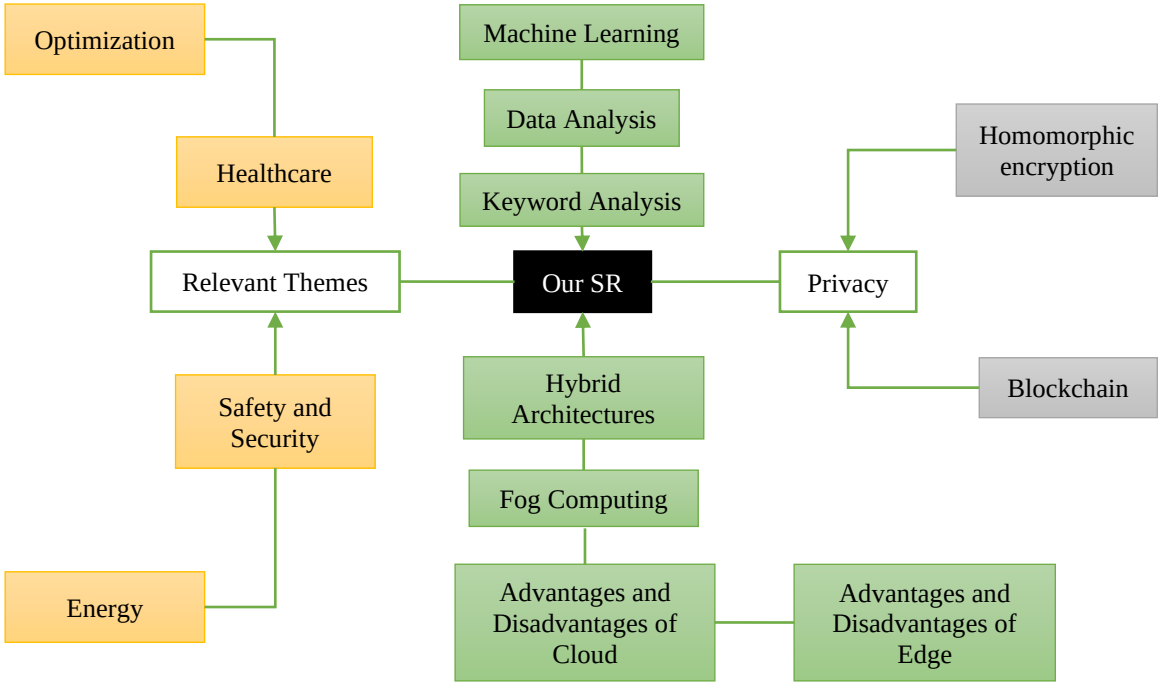

Fig 5. Structure of this SR

Bibliometric Assessment

Fig. 6 illustrates the range of release dates categorized by month. The range is generally consistent, indicating that this issue is not exclusively associated with a single time of year or any particular occurrence. Notwithstanding this, we saw a rise in releases pertaining to blockchain, fog computing, and healthcare in 2023 relative to 2022.

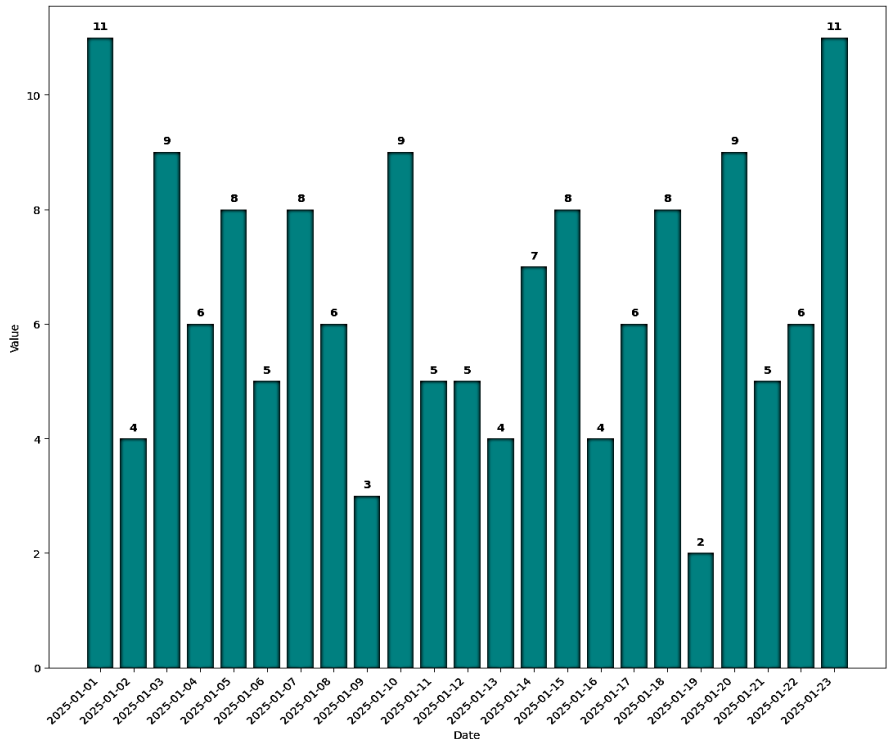

Fig 6. Monthly Count of Analyzed Articles

Keyword Analysis

Following the selection of the articles, we examined the keywords used in each one; using this data, we constructed several graphs to elucidate the subjects most closely associated with edge computing or cloud computing. A keyword cloud is illustrated to provide a visual overview of the keywords employed in the articles for a preliminary examination. A keyword cloud is an image composed of words, with the prominence and size of every keyword indicating its range in the examined keyword list. **Fig. 7** illustrates the keyword cloud produced from the categories extracted from the examined texts. As

anticipated, based on the employed study string, the keywords "IoT" (acronym for Internet of Things) and "edge" (abbreviation for edge computing) are predominant among the others.

Fig. 7 illustrates that "cloud" ranks as the third most prevalent phrase, suggesting that most articles examine it in relation to "edge". Moreover, security and privacy are paramount; indeed, the majority of the benefits of "edge" are linked to safeguarding user security and privacy. Local data processing on endpoint units prevents transmission to distant servers, over which the user lacks control. Given the constrained computing capacity of endpoint units relative to the cloud, the terms task offloading, latency, and resource management become salient; this indicates that several studies investigate strategies for enhancing processing power efficiency and storage at the edge.

Fig 7. Keyword Cloud Produced from the Keywords of Reviewed Articles

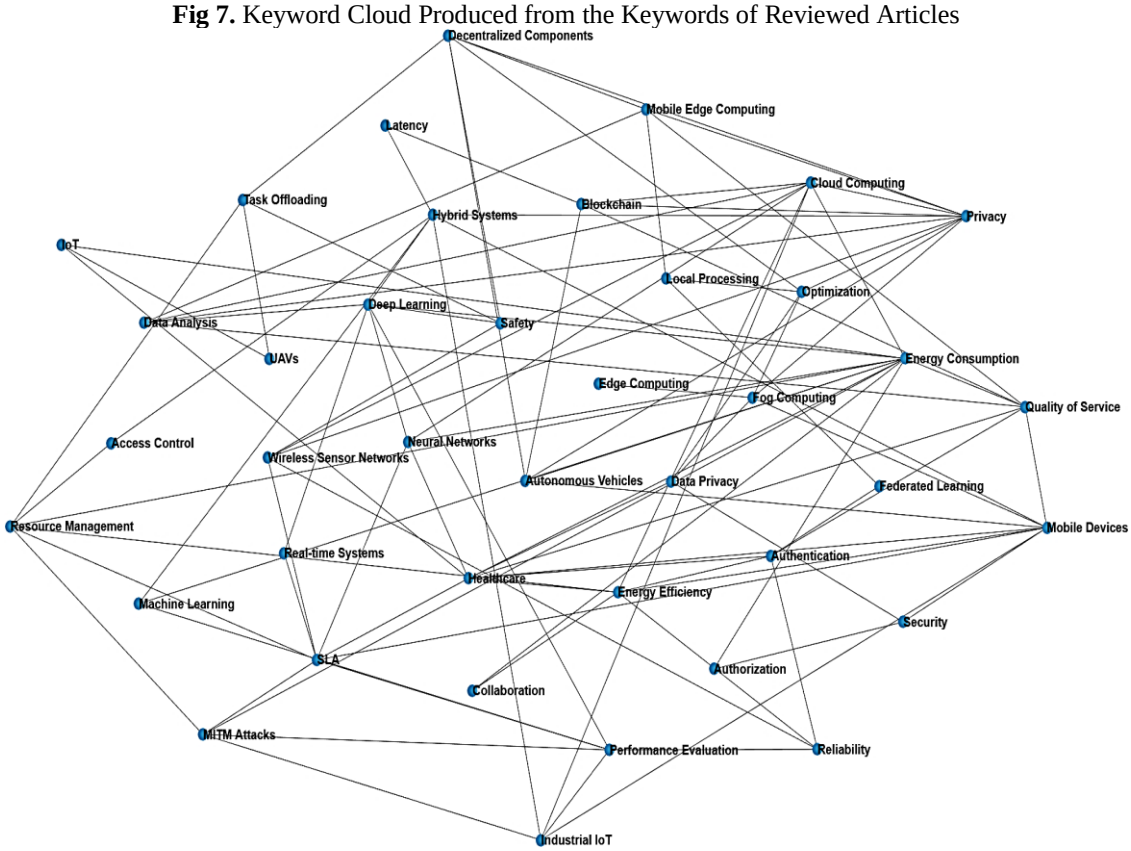

Fig 8. Keyword Co-Occurrence Network

To evaluate the interactions among the subjects that were evaluated in the articles, we developed an association map, illustrated in **Fig. 8**, known as a keyword co-occurrence matrix. An immersive and flexible association map may be analyzed utilizing Gephi program, or Cytoscape, by acquiring the keyword file accessible on GitHub. The map depicts keywords as blue dots of differing sizes based on the rate, while the colorful lines denote the links between distinct themes.

The network illustrates the significant association between the IoT and numerous other subjects, affirming the pervasiveness of this approach in the contemporary scene. Fog computing nodes are significant, suggesting that several articles advocate for hybrid edge-cloud systems. Terms like machine learning, deep learning, and federated learning are intricately linked to one another and to other ideas. These approaches are employed to assess the substantial amount of data generated by IoT tools. Based on the last 3 sub-questions of the cluster structure, all labels pertinent to IoT and edge computing were examined, resulting in the proposal of two distinct histograms.

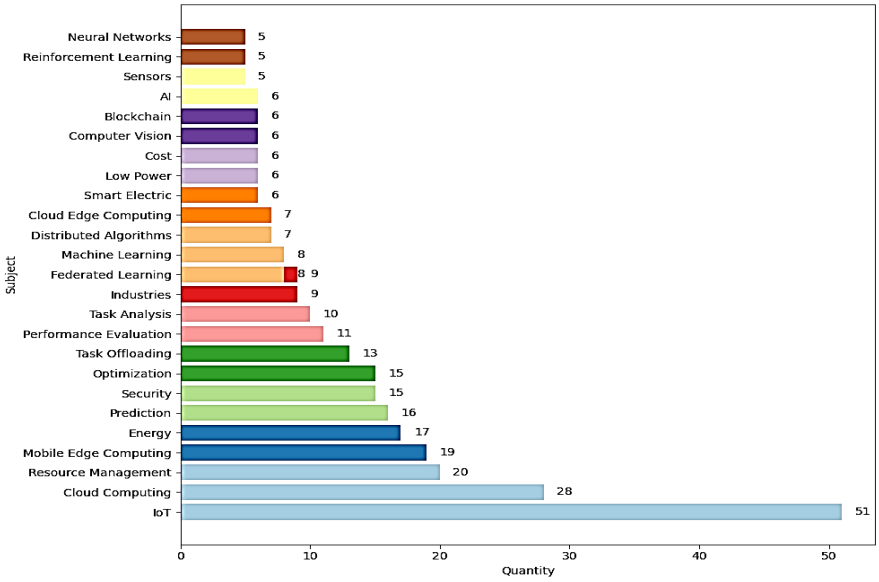

Fig 9. Subjects Linked to Edge Computing

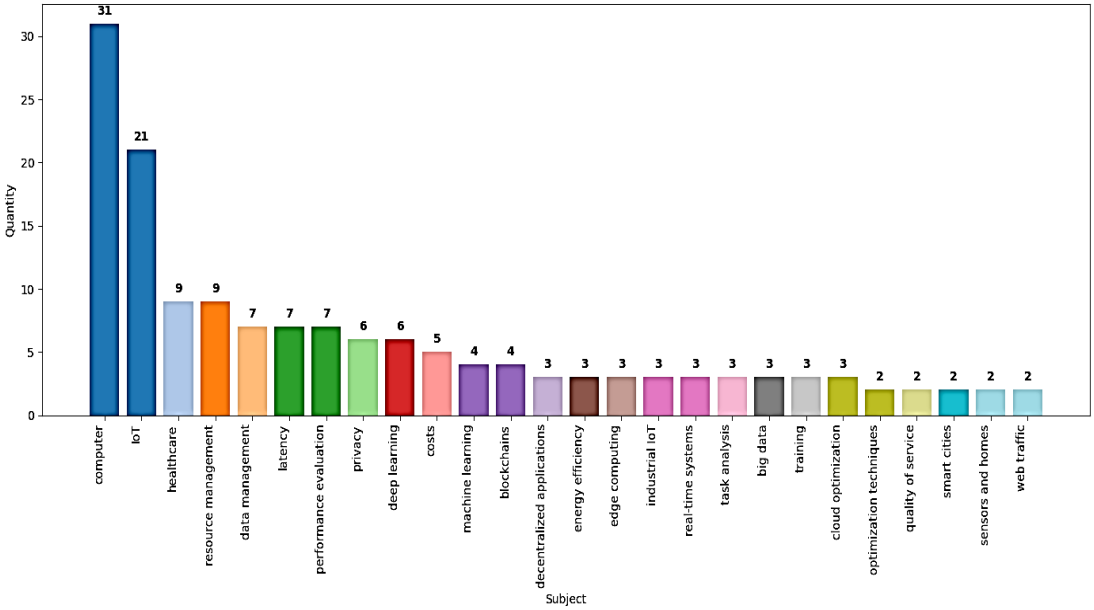

Fig 10. Subjects Related to Cloud Computing

The histogram of subjects associated with edge computing, illustrated in **Fig. 9**, reveals that the most relevant keywords are cloud computing and IoTs: IoT devices perform optimally when integrated with an intermediary layer for data processing and workloads control, subsequently delegating more intensive tasks to the cloud. Edge computing layer incorporation enhances the power efficiency of IoT tools and fortifies the overall infrastructure safety. **Fig. 10** illustrates the histogram of subjects associated with cloud computing, highlighting its uses. The majority of the examined publications include the keywords “IoT” and/or “edge computing”. A pertinent subject concerning cloud computing is latency, since several studies examine the challenges associated with network delay, an area where hybrid solutions and edge computing might mitigate the issue.

Issues and Application Cases

The documents were methodically gathered and examined to discern and classify the many applications of edge computing. This facilitated our comprehension of the applications of edge computing. This investigation uncovered a diverse array of applications for this nascent technology over several areas, illustrating its capacity to influence countless facets of our lives.

Herein, we explore certain themes of interest pertinent to this review. This encompasses an examination of 3 essential issues: resource management, safety, and security. Subsequently, we examine a particular application case that illustrates the efficacy of edge computing: healthcare.

Safety and Security

Cloud-edge infrastructures provide significant capabilities; yet, each layer is susceptible to malicious attacks aimed at acquiring sensitive data or disrupting service operation. The paramount security dangers pertain to network endpoint assaults, such as breaches in access control systems, which target the authentication and authorization mechanisms between edge computers and IoT nodes, as well as between cloud services and edge computers. This method enables the extraction of data from the infrastructure or the injection of malicious code, using vulnerabilities introduced by the existing deployment. A further revealed aspect of the design is the communication channel: Ensuring secure data flow is crucial; moreover, the identities of both ends must be authenticated, and the pathway must be protected against eavesdropping attacks. A MITM assault transpires when an intermediary, C, impersonates endpoint A to endpoint B and vice versa during their conversation.

Consequently, even if all packets are properly delivered to the terminals, the data remain vulnerable to C. This occurs especially when the payloads are sent in plain text and lacks a robust authentication mechanism to validate the authenticity of the endpoints. Specialized authentication techniques may mitigate common issues associated with IoT devices, hence decreasing computational and communication expenses. A significant safety issue is the dependability of the design, ensuring that a system remains operational despite the failure of one or more components. A potential method to enhance reliability is the use of decentralized components, such as blockchain technology for data storage and protected access; this approach augments the architecture's resilience and eliminates a single point of failure.

Resource Management

Evaluating the computational and storage expenses of an architecture is essential. Given the substantial amounts of data requiring analysis and storage, optimizing resource utilization and allocation is imperative. A multitude of research publications investigate optimum resource management strategies. When designing architecture that incorporates IoT devices, it is essential to account for the energy factor due to their need on battery power. Numerous variables affect energy consumption, such as CPU utilization, the frequency of sensor data collection, and the frequency of data transfer across the network. Regarding energy consumption, it is sometimes advantageous to refrain from executing certain operations on IoT devices, particularly those that are CPU-intensive, and to assign another component within the architecture to do that processing. Energy concerns are essential for building an autonomous aerial vehicle-based edge computing system, since the on-boarding energy is allocated between the computing system and the drone’s components (navigation, motors, etc.).

An effective method to optimize devices' processing capabilities is via the use of task-offloading techniques. These algorithms systematically allocate tasks across several nodes, enhancing user experience, and reducing latency. They use a dynamic methodology, allocating tasks to either a more rapid node or one with a reduced workload. This guarantees a reduction of bottlenecks, and optimization of resources. Another objective for these techniques is to reduce both energy usage and service latency. A workload controller implementing a task-offloading technique must assess whether a task may be effectively performed on the IoT devices, given its constrained computing resources, or if it is more advantageous to offload it to an endpoint, which may subsequently pass tasks to the cloud nodes. These techniques may also use hierarchical reinforcement learning, enabling the task delegation model to enhance progressively over time.

An alternative method to address the energy constraints of IoT devices is to include power harvesting capabilities into the infrastructure: stationary tools (e.g., network hotspots) are configured to provide portable smart devices both power source and computational assistance (based on offloading). Performance assessment is often employed to guarantee the adherence to SLA (service-level agreements) via the operational phase of the infrastructure. By monitoring measures such as expenditure, service velocity, data utilization, CPU use, and energy consumption, an architecture engineer may proactively detect and rectify possible faults. This methodology guarantees that the design reliably fulfils its performance and resource efficiency objectives.

Healthcare

IoT and edge computing have transformed the clinical industry, allowing treatment outside traditional hospital facilities. This is feasible because to MEC (mobile edge computing), a decentralized framework designed to link mobile devices such as tablets and smartphones with the cloud via peripheral nodes. This harnesses the advantages of mobile device and sensor data functionalities, augmented by the computing power of the cloud. Edge nodes are capable of managing essential tasks that need minimal delay, while cloud feedback times are inadequate. IoTs tools are frequently employed in the medical sector to gather data on patients' ailments. AI analysis may analyze data from sensor devices and provide data beneficial for patients and physicians.

V. CONCLUSION

We have studied how cloud computing and edge computing can be combined in the Internet of Things (IoT). We review key points of these architectures with regard to the enhancement of the safety, effectiveness, and scalability of IoT systems mostly in relation to the medical field, resource management, and privacy issues. The focus on the hybrid approaches like fog computing has reinforced the usefulness of this type of solution in dealing with problems like latency, energy

consumption, and work distribution. Moreover, bibliometric and keyword analysis has explained the patterns of development and future technologies in this field, such as federated learning and blockchain, that are redefining future IoT systems. Notwithstanding such success, there is an issue of security loopholes and resource provisions of an edge-cloud that should blend smoothly with other resources that need to be managed.

CRediT Author Statement

The author reviewed the results and approved the final version of the manuscript.

Data Availability

The datasets generated during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interests

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Funding

No funding was received for conducting this research.

Competing Interests

The authors declare no competing interests.

References

[1]. W. Choi, T. Choi, and S. Heo, "A comparative study of automated machine learning platforms for exercise Anthropometry-Based Typology Analysis: performance evaluation of AWS SageMaker, GCP VertexAI, and MS Azure," Bioengineering, vol. 10, no. 8, p. 891, Jul. 2023, doi: 10.3390/bioengineering10080891.

[2]. H. El-Sayed et al., "Edge of Things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment," IEEE Access, vol. 6, pp. 1706–1717, Dec. 2017, doi: 10.1109/access.2017.2780087.

[3]. Y. Zhang, "Research and application of next-generation firewall technique in medical network," Journal of Computational Methods in Sciences and Engineering, vol. 22, no. 5, pp. 1461–1476, Jun. 2022, doi: 10.3233/jcm-226182.

[4]. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of things: architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, Mar. 2017, doi: 10.1109/jiot.2017.2683200.

[5]. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, Jan. 2015, doi: 10.1109/comst.2015.2444095.

[6]. T. K. L. Hui, R. S. Sherratt, and D. D. Sánchez, "Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies," Future Generation Computer Systems, vol. 76, pp. 358–369, Nov. 2016, doi: 10.1016/j.future.2016.10.026.

[7]. N. Cvar, J. Trilar, A. Kos, M. Volk, and E. S. Duh, "The use of IoT technology in smart cities and smart villages: similarities, differences, and future prospects," Sensors, vol. 20, no. 14, p. 3897, Jul. 2020, doi: 10.3390/s20143897.

[8]. Ren, D. Zhang, S. He, Y. Zhang, and T. Li, "A survey on End-Edge-Cloud Orchestrated Network Computing Paradigms," ACM Computing Surveys, vol. 52, no. 6, pp. 1–36, Oct. 2019, doi: 10.1145/3362031.

[9]. G. Suciu et al., "Big data, internet of things and cloud convergence – an architecture for secure E-Health applications," Journal of Medical Systems, vol. 39, no. 11, Sep. 2015, doi: 10.1007/s10916-015-0327-y.

[10]. C.-L. Hsu and J. C.-C. Lin, "An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives," Computers in Human Behavior, vol. 62, pp. 516–527, Apr. 2016, doi: 10.1016/j.chb.2016.04.023.

[11]. T. J. Gerpott, N. Ahmadi, and D. Weimar, "Who is (not) convinced to withdraw a contract termination announcement? – A discriminant analysis of mobile communications customers in Germany," Telecommunications Policy, vol. 39, no. 1, pp. 38–52, Jan. 2015, doi: 10.1016/j.telpol.2014.11.005.

[12]. U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive review," Sensors, vol. 23, no. 8, p. 4117, Apr. 2023, doi: 10.3390/s23084117.

[13]. Fiannaca, M. La Rosa, R. Rizzo, A. Urso, and S. Gaglio, "An expert system hybrid architecture to support experiment management," Expert Systems With Applications, vol. 41, no. 4, pp. 1609–1621, Sep. 2013, doi: 10.1016/j.eswa.2013.08.058.

[14]. W. Villegas-Ch, J. Govea, R. Gurierrez, and A. Mera-Navarrete, "Optimizing security in IoT ecosystems using hybrid artificial intelligence and blockchain models: a scalable and efficient approach for threat detection," IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2025.3532800.

[15]. P. Phalaagae, A. M. Zungeru, A. Yahya, B. Sigweni, and S. Rajalakshmi, "A Hybrid CNN-LSTM Model with Attention Mechanism for Improved Intrusion Detection in Wireless IoT Sensor Networks," IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2025.3555861.

[16]. F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge Computing and Cloud Computing for Internet of Things: a review," Informatics, vol. 11, no. 4, p. 71, Sep. 2024, doi: 10.3390/informatics11040071.

[17]. P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1078–1124, Jan. 2021, doi: 10.1109/comst.2021.3062546.

[18]. H. Sodhro, Z. Luo, A. K. Sangaiah, and S. W. Baik, "Mobile edge computing based QoS optimization in medical healthcare applications," International Journal of Information Management, vol. 45, pp. 308–318, Sep. 2018, doi: 10.1016/j.ijinfomgt.2018.08.004.

[19]. Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal Pricing-Based Edge Computing Resource Management in Mobile Blockchain," 2018 IEEE International Conference on Communications (ICC), May 2018, doi: 10.1109/icc.2018.8422517.

[20]. C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on FoG Computing: State-of-the-Art and Research challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 416–464, Nov. 2017, doi: 10.1109/comst.2017.2771153.