

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 12, April 2025



A Review of Security Issue when Integrating IoT with Cloud Computing and Blockchain

Mr. Thangadurai K¹, Sathish Kumar T², Suresh D³, Balamurugan U⁴, Karuppuchamy⁵

Assistant Professor, Computer Science and Engineering¹ Students, Computer Science and Engineering²⁻⁵ Mahendra Institute of Engineering and Technology, Namakkal, India

Abstract: The integration of the Internet of Things (IoT) and cloud computing, which play essential roles in our everyday routines, is expected to emerge as a fundamental element of the forthcoming internet, realizing increased usage and acceptance. This fusion is anticipated to revolutionize various applications, offering The integration of IoT and cloud may pose challenges. Cloud computing's capacity to distribute resources and data across diverse locations, facilitating access from different industrial settings, has significantly enhanced IoT functionality. However, rapid migration to the cloud has raised security concerns, as conventional security measures for computers are not always applied effectively to cloud-based systems. Overcoming these obstacles can be achieved by integrating cloud and IoT technologies, as the vast resources available on the cloud can greatly benefit IoT, helping the cloud transcend current limitations related to physical objects in a more dynamic, distributed manner. Several discoveries from the research were made by exploring the facilitation of a smooth shift of IoT initiatives to the cloud by studying IoT and cloud computing, investigating various cloud-related challenges and resolutions derived from recent scholarly works, and analyzing the most recent advancements in attacks targeting cloud-based IoT systems. Identifying gaps in the research on IoT-based cloud infrastructure and addressing cybersecurity in cloud computing is important for future research directions, necessitating a review of the technological challenges mentioned in the literature. As such, this research explores how blockchain technology effectively addresses security concerns within this combination, emphasizing its capacity to improve data integrity and privacy and to ensure secure transactions. The exploration delves into the multifaceted implications and potential applications of blockchain, elucidating its role in reinforcing the overall security of these interconnected systems

Keywords: Internet of Things

I. INTRODUCTION

Combining Internet the of Things (IoT) and cloud computing offers a fast method of managing, storing, and understanding data collected from IoT devices. It allows devices to send their data to the cloud, where it can be easily stored and analyzed Using cloud computing makes it easier and cheaper for people and businesses to set up and use many connected devices. Thus, bringing together IoT and cloud The associate editor coordinating the review of this manuscript and approving it for publication was Nitin Gupta.

computing has enabled the creation of systems that turn data from sensors and devices into things we can do or decisions we can make. This combination also helps with predictions and quick decision-making by watching things happen in real-time. It also helps identify problems throughout the whole system. Moreover, in cloud-based applications, it is simple to adjust the size of what you are using at will because hardware and software tasks are handled separately Ensuring data is safe and private when sent between IoT devices and the cloud is achieved by using end-to-end encryption protocols. In addition, cloud computing allows the offloading of computer tasks, speeding up processes and reducing the time it takes to process information Bringing these technologies together offers many benefits, such as better performance, the ability to grow easily, predict what might happen, saving money, greater security, and more convenience First and foremost, putting these things together really boosts how well everything

Copyright to IJARSCT www.ijarsct.co.in



DOI: 10.48175/IJARSCT-25983





International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 12, April 2025



works by simplifying device connection and data sharing without issue. The significant computing power and storage space in the cloud handle much data from IoT devices very efficiently, ensuring everything is processed and viewed smoothly. Being able to easily adjust to different needs easily is a significant advantage in this combination, thanks to the cloud's ability to change its resources as needed. This ability to adjust easily is especially good for IoT applications because the number of connected devices can increase or decrease often. In addition, the power of prediction is improved. By using the information, we obtain from IoT devices and using smart math in the cloud, organizations can figure out important things, offer predictions, and make smart decisions. This helps with caring for things before they break, improving processes, working better, and even anticipating customer and market actions. It also saves much money. The cloud's policy of paying only for what you use allows companies to avoid spending significant money upfront on necessities to get started. As well, IoT devices do not need much storage and computer power on their own because the cloud accounts for a significant part of the work, cutting down the costs for each device. Combining technologies work together like this also strengthens security much, as the cloud usually has solid safety features, such as keeping information safe with codes, controlling who has access, and updating things regularly to remain safe, improving the security of IoT systems significantly. The cloud can watch over and control many connected devices all in one place, simplifying the search and destruction of any security problems that might occur. The user experience is also simplified, as they can reach and control their IoT devices and the information they collect from anywhere using applications or platforms in the cloud. These remote capabilities make it easy to watch, control, and understand IoT systems, allowing everything to work better and to become more adaptable. Thus, bringing together IoT and cloud computing is a significant change that brings many benefits to different areas.

The IoT, which is akin to a significant web of connected devices and sensors, holds much data that requires ample computer power to store, process, and understand. As such, cloud computing enables the obtainment of the right amount of computer power easily when we need it, making it efficient to deal with all this data. This combination makes it easy to combine everything together, enabling quick movement, storage, and understanding of real-time data. This also con- tributes to better decision-making and improved predictions, as the cloud's centralized system makes it easier to obtain, secure, and control the data the IoT creates. Combining

IoT and cloud computing thus allows us to create new and creative applications and services, pushing forward such areas as healthcare, smart cities, and industrial automation. Through this combination, not only does everything work more efficiently, but it also encourages new ideas, and growth in many different areas is encouraged However, combining IoT and cloud computing has also brought many security concerns. For instance, data breaches and privacy problems can occur because of all the connections and shared information between devices and cloud networks. Dealing with these tricky security problems therefore necessitates creative solutions, one powerful example of which is using blockchain technology, which can help strengthen security in this connected system. Recognized for being decentralized, resistant to tampering, and transparent, blockchain becomes a hopeful solution to fix security problems brought by combining IoT and cloud computing. In response, this paper looks at how blockchain technology could play a crucial role in improving security in this integration. It assesses how blockchain can ensure data stays true, maintains privacy, and makes transactions secure, rendering the whole security system stronger for these connected systems.

Companies using connected devices can gain much from combining IoT and cloud computing, the latter of which allows for quick and safe storage, processing, and access to data from IoT, meaning we can implement automation, analyze information, and make better decisions by collecting and studying real-time data on a larger scale

This research paper investigates the collaboration of IoT, cloud computing, and blockchain, first by detailing how IoT and the cloud work together to simplify the management of data from various devices. This partnership facilitates speedy data processing, storage, and analysis, making it a significant tool because it enhances decision-making and enables accurate predictions. However, in combining these technologies, combined, there are security concerns that have been expressed. To address them, the paper examines blockchain technology, recognized for its decentralized, transparent, and secure nature. This study seeks to explore its potential to enhance the security of IoT and cloud computing. It also aims to determine whether blockchain can contribute to strengthening data security, safeguarding privacy, and ensuring secure transactions within these systems. Finally, the research endeavors to ensure the safety and security of IoT and Cloud Computing when combined. The study's objectives can be summarized as follows:

Copyright to IJARSCT www.ijarsct.co.in



DOI: 10.48175/IJARSCT-25983





International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 12, April 2025



To explore how IoT, cloud computing, and blockchain technologies can be combined and work together.

To highlight the benefits of combining IoT and cloud computing for data processing, scalability, making predictions, and cost savings.

To identify the growing security issues within interconnected networks of IoT and cloud systems. To investigate how blockchain technology can strengthen security within this integrated ecosystem.

To examine how blockchain improves data integrity, privacy measures, and transaction security through the integration of IoT and cloud computing.

This study makes significant contributions to the literature on integrating IoT, cloud computing, and blockchain. By thor- oughly examining the combination of these technologies, the research will clarify the complex dynamics and implications, providing a roadmap to improve the collaboration between IoT and the Cloud while incorporating Blockchain for enhanced security. Such insights are invaluable, benefiting the field by deepening our understanding of how these technologies intersect and offering strategies to tackle the emerging security concerns linked to their integration. Furthermore, this study will be of great value to future investigations, providing a strong foundation for subsequent researchers entering this domain. Future researchers can also use the findings of this study to delve deeper into security aspects, exploring various applications of blockchain technology and innovative methods to strengthen the security of integrated IoT and cloud computing systems. The significance of this study lies in its potential to lead the revolution toward the more secure, efficient, and optimized utilization of these technologies in various domains. Finally, conducting this research is crucial to ensuring that the integration of IoT, cloud computing, and blockchain progresses in a secure, reliable, and transformative manner, driving innovation and progress across various sectors.

This paper uniquely explores the combination of IoT, cloud computing, and blockchain technologies, highlighting its innovative approach in comparison to existing studies. Unlike other research that might examine these technologies separately, this paper focuses on how they can work together effectively, with a special emphasis on improving security. In addition, it thoroughly investigates how the core features of blockchain, such as decentralization, transparency, and strong security, can enhance the integration of IoT and cloud computing. This study is extensive, covering not just technical details but also such benefits as scalability, cost savings, and improved predictive analytics, which are crucial to applying these technologies in real-world scenarios. Further, it provides recommendations to address new security risks that arise from connecting these systems. This forward-looking approach distinguishes the paper, making it a critical resource for future research and offering a roadmap for navigating the complexities of integrating these technologies safely and efficiently.

This study thoroughly assesses how IoT, cloud computing, and blockchain can work together, as divided into different parts to help in understanding it better. Section clarifies how we select and analyze the papers and studies that are relevant to ours using the PRISMA 2020 flow diagram. In Section , we begin by exploring the fundamentals of IoT and cloud computing. We will discuss IoT technologies, protocols, architectures, limitations, and suggested security practices. Thereafter, we moved on to cloud computing, where we explained service and deployment models.

After that, we delve into how IoT can be integrated with cloud computing. The Discussion section (Section) represents the core of this paper, where we dive into the complex challenges related to security in IoT and the cloud. We also discussed important topics, including service quality, identity management, data security, support protocols, resource allocation, big data handling, energy consumption, and computational performance. In this section, we will focus on how blockchain can strengthen the integration of IoT and cloud computing, especially in dealing with security issues. The Related Studies (Section), Open Challenges and Lim- itations (Section), and Future Directions (Section), these sections are like a road map for future research, shedding light on what has already been studied, areas seldom explored, much, and potential paths toward progress. Finally, in the Conclusion (Section) we summarize the important findings, highlighting how blockchain plays a crucial role in securing the integration of IoT and the cloud and we suggest future research directions to make security even stronger in this combined area.

Copyright to IJARSCT www.ijarsct.co.in



DOI: 10.48175/IJARSCT-25983



International Journal of Advanced Research in Science, Communication and Technology



International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 12, April 2025



SELECTION OF RESEARCH PAPERS FOR REVIEW

A systematic literature review (SLR) is a crucial research method used to thoroughly explore revolution previous research and studies on a particular topic. Its primary goal is to gather a complete collection of relevant papers in said field. This serves as an effective way of bringing together past findings and filling any gaps in our knowledge. With the increasing amount of research and scientific papers, there is a rising need for a dependable and strong study that summarizes previous work and combines these findings to address any identified gaps.

In our research paper, we used the PRISMA 2020 Flow Diagram designed for new systematic reviews (shown in Figure) to demonstrate visually how many records were included or excluded when selecting studies. We started by searching for relevant research papers on Google Scholar, using a specific search string related to "Security OR security and privacy AND issues OR obstacles OR problems AND Integration AND IoT AND Blockchain OR Internet of Things AND Cloud OR Cloud Computing OR computing architecture." This initial search resulted in an initial count of 525 papers. After refining the search, removing duplicates, and using automation tools to exclude irrelevant entries, the total was reduced to 267. Following these steps, we were left with 258 records. Further screening helped us identify and exclude 179 reports that were either irrelevant to the main topic, not written in English, or not presented in a journal or conference format. This brought the final countdown to 72 remaining reports.

BACKGROUND

In recent times, both cloud computing and IoT have become prominent as leading technologies, a fact supported by research findings The current trend suggests rapid growth in digital technology, and the coming together of FIGURE 1. Selection of papers for literature review using PRISMA.

cloud computing and IoT holds the potential for efficient resource management. In this section, we first review the various types, architectures, and deployment models of cloud computing. Furthermore, we delve into security concerns and challenges linked to these models. The collaboration between IoT and cloud computing acts as a powerful team in today's technology landscape. IoT devices, ranging from sensors to smart gadgets, generate substantial data, but handling and interpreting all these data can be challenging. Hence, by integrating IoT with cloud computing, we solve this challenge Cloud computing involves using large, distant computers to store and process data. Thus, when we link IoT to these remote servers, it helps us manage data more effectively. Cloud servers can handle a substantial amount of data generated by IoT devices, store them, process them, and enable quick analysis. This connection is extremely beneficial for businesses, allowing them to make faster decision-making based on real- time information. It also ensures data accessibility from anywhere, benefiting industries, such as healthcare, manufacturing, transport, and smart cities. The collaboration between IoT and cloud computing therefore enhances technology, making it smarter and more efficient and transforming how we solve problems and innovate

Blockchain technology could play a crucial role in improving the integration of IoT and cloud computing, functioning as a digital ledger that securely stores information across a network of computers, making it extremely difficult to alter or hack When integrated with IoT and cloud computing, blockchain can provide an additional layer of security and trust in the data generated by IoT devices.

For example, IoT devices continuously gather sensitive data, such as personal information or critical operational data. By using blockchain, these data can be securely recorded and verified. The decentralized nature of blockchain ensures that the data are not stored in a single location, reducing vulnerability to cyber-attacks In addition, it guarantees data integrity and authenticity of the data. Each piece of information stored on the blockchain is timestamped and linked to previous records, forming a transparent and unalterable history of the data's journey.

Furthermore, blockchain technology allows the implemen- tation of smart contracts, which are self-executing contracts with terms directly written into code. These contracts can automate processes between IoT devices and cloud services without requiring a central authority, diminishing the need for intermediaries, and boosting efficiency in transactions or interactions.

In simple terms, incorporating blockchain into IoT and cloud computing offers an extra layer of security, transparency, and efficiency to the system As well, it assists in securing sensitive data, ensuring their authenticity, and automating processes, thereby enhancing the overall trustworthiness and reliability of the entire system.

Copyright to IJARSCT www.ijarsct.co.in



DOI: 10.48175/IJARSCT-25983





International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 12, April 2025



ΙΟΤ

Anything located on the Earth's surface, whether it is an interactive device or a non-interactive object, falls under the category of a "thing" in the IoT, which represents a revolutionary concept where forming an extensive network of interconnected devices and objects capable of com- municating and sharing data without human intervention. This includes a wide range of everyday items, from smart thermostats and wearable fitness trackers to industrial sensors and autonomous vehicles, all linked through the internet. Thus, the significance of the IoT lies in its transformative ability to connect the physical and digital worlds, facilitating seamless communication and empowering these devices to collect, exchange, and act on data This interconnected ability will bring convenience and efficiency to our lives and industries, and by integrating sensors, actuators, and communication capabilities into various objects and systems, IoT facilitates automation, real-time monitoring, and intelli- gent decision-making as well as streamlines processes, optimizes resource utilization, enhances productivity, and creates new opportunities across various sectors such as manufacturing, transportation, agriculture, and smart cities. As IoT continues to evolve, its capacity to connect devices and provide data-driven insights holds the potential to unlock innovative solutions and shape a more connected and efficient world

TECHNOLOGIES EMBEDDED IN IOT DEVICES

Sensors:

They are like the eyes and ears of smart devices in the IoT. They work on collecting real-world data. For example, to detect room temperature, regardless of whether it is getting hotter or colder, to keep an eye on movement; or to check the humidity, sensors gather all details. This helps devices determine what is happening in their surroundings. In terms of security, sensors can read unusual activities or sudden changes. For example, they might alert you if someone is trying to access a device without permission or if there is a shift in the environment that could affect how the device works

Actuators:

Actuators are like the actors in smart devices. They do things based on what the sensors tell them. Whether it is turning something on or off or making things move, actuators follow the instructions they are given. In terms of security, actuators can keep things safe by acting when a sensor raises an alarm. For example, they could lock a door or stop a system if there is a security problem

Network:

The network provides connectivity which is how smart devices communicate with each other or with a main system. For example, they use Wi-Fi, Bluetooth, or cell networks to send and receive data [17], [18]. From a security perspective, it is crucial to use strong encryption methods to secure communication between devices and servers. This helps stop unauthorized access and keeps important information safe while it is moving around [19].

IOT ARCHITECTURE

Through data communication methods, particularly via radio frequency identification (RFID) tags, these objects transition into communicative nodes capable of exchanging information across the internet. The traditional IoT architecture consists of three core layers: the perception layer, the network layer, and the application layer. However, some sources [20], [21] have introduced the middleware and the business layers as additional components supplementing the existing three layers, resulting in the formation of a comprehensive five-layer architecture, as illustrated in Fig. 2: The architecture of IoT architecture consists of five like Man-in-the-Middle (MitM) or denial-of-service (DoS) attacks [22]. The third layer, called the middleware layer, handles such tasks as processing data, storing information, and managing devices. In terms of security, it is important to ensure that the data remains intact, are encryption is utilized when sending and storing, and prevent unauthorized access to stored information is prevented.

Copyright to IJARSCT www.ijarsct.co.in



DOI: 10.48175/IJARSCT-25983





International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal



Moving on to the application layer, here, user applications and services connect with IoT systems. Security concerns here include ensuring that authentication (verifying identity) is secure, authorization (controlling access) is reliable, and application programming interface (API) interactions are secure to avoid any exploitation of application vulnerabilities [23]. Finally, the business layer manages business applications, analytics, and decision-making processes, and its security is centered on safeguarding sensitive business data, ensuring the operations comply with regulations, and setting up secure access controls for critical business functions [12].

II. DISCUSSION

There is a strong interconnection between the IoT and cloud computing, as each technology is considered supportive and complementary to the other technology. The IoT provides the ability to collect data from multiple devices and thus the ability to analyze significant data, while cloud computing provides huge resources to store, process, manage data, and improve the security of this data. Recently, these technologies have been depended upon within the tech-nological landscape to develop decision-making processes, improve operations, and enable competition in various institutions [60].

For successful integration of cloud and IoT, various issues must be addressed to ensure benefits for the wider population. While the fusion of Cloud and IoT opens up numerous opportunities and possibilities, it also presents an expanded target for potential attackers. The integration involves diverse data types and services supported by multiple networks that require a flexible network structure capable of supporting a wide array of data and fulfilling quality of service require- ments [32]. Addressing protection concerns is most important to prevent unauthorized admission of user information. The integration of IoT with cloud computing introduces a multitude of complicated protection challenges

RELATED STUDY

The forthcoming section aims to explore and analyze recent studies and developments pertaining to the integration of IoT and cloud computing, with a specific focus on the role of blockchain technology within this amalgamation. This segment dives into insightful works, investigative papers, and observational pieces to uncover the complexities and progres- sions in consolidating IoT and cloud computing standards. It scrutinizes the advancing environment of this integration, highlighting challenges, opportunities, and suggestions for various businesses and spaces. In addition, it covers the progressive utilization of blockchain, as a significant enabler of advancing the security, versatility, and decentralization components of IoT and cloud integration. By synthesizing findings from recent studies, this section

Copyright to IJARSCT www.ijarsct.co.in



DOI: 10.48175/IJARSCT-25983



584

Impact Factor: 7.67



International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal



Volume 5, Issue 12, April 2025

endeavors to offer a comprehensive understanding of the synergies among IoT, cloud computing, and blockchain, shedding light on their collaborative potential to revolutionize diverse sectors and pave the way for more secure and efficient interconnected ecosystems.

This section thoroughly examines various important aspects related to the integration of IoT and cloud computing, particularly focusing on security issues. It covers such topics as technology, deployment, service, and sector/application, as well as the problems that have been discussed in this field. It also considers future opportunities and any limitations we might encounter. Moreover, the section explores how mobility plays a role within this context, the goal of which is to provide a clear understanding of the challenges and complexities involved in merging IoT and cloud computing while maintaining security.

OPEN CHALLENGES AND LIMITATIONS

While the integration of IoT, cloud computing, and blockchain technology presents a promising approach to bolstering security, several limitations persist. One primary concern involves the computational overhead and energy consumption associated with blockchain implementation in large-scale IoT networks. The consensus mechanisms within blockchain systems often demand extensive computational power, potentially hindering the scalability and performance of IoT devices with limited resources. Moreover, the inte- gration of these technologies introduces complexity, leading to interoperability challenges and potential vulnerabilities stemming from the complex interactions between diverse systems. Additionally, the regulatory landscape and compliance standards are evolving, raising uncertainties around legal and regulatory frameworks governing the use of blockchain in different sectors. Security concerns such as potential privacy breaches, data management, and identity verification in a decentralized environment remain open challenges that require extensive research and robust solutions. Furthermore, while blockchain offers immutable and transparent ledgers, it is not immune to all security threats, such as 51 percent attacks and novel cryptographic vulnerabilities, necessitating continuous evolution and adaptation of security measures in this integration. Addressing these limitations will be crucial in realizing the full potential of integrating IoT, cloud computing, and blockchain while ensuring robust security.

III. CONCLUSION

IoT and cloud technologies have experienced remarkable growth in recent times. Moving forward, IoT and cloud systems are expected to generate vast volumes of data that necessitate efficient collection and processing. Secu- rity stands out as one of the most significant challenges confronting the realms of cloud computing and IoT. This paper delves into investigating the amalgamation of IoT and cloud computing, addressing issues compatible with cloud systems and computing methodologies to facilitate the smooth transition of IoT applications to the cloud.

REFERENCES

[1] A. Mohiyuddin, A. R. Javed, C. Chakraborty, M. Rizwan, M. Shabbir, and J. Nebhen, "Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system," Int. J. Fuzzy Syst., vol. 24, no. 2, pp. 1203–1215, Mar. 2022.

[2] Y. Karam, T. Baker, and A. Taleb-Bendiab, "Security support for intention driven elastic cloud computing," in Proc. 6th UKSim/AMSS Eur. Symp. Comput. Modeling Simulation, Nov. 2012, pp. 67–73.

[3] L. Golightly, V. Chang, Q. A. Xu, X. Gao, and B. S. Liu, "Adoption of cloud computing as innovation in the organization," Int. J. Eng. Bus. Manage., vol. 14, Jan. 2022, Art. no. 184797902210939.

[4] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber security in IoT-based cloud computing: A comprehensive survey," Electronics, vol. 11, no. 1, p. 16, Dec. 2021.

[5] D. CeArley, B. Burke, S. Searle, and M. J. Walker. (Oct. 3, 2017). Gartner's top 10 Strategic Technology Trends for 2017. Accessed: Feb. 5, 2020. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018





DOI: 10.48175/IJARSCT-25983





International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 12, April 2025



[6] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future Gener. Comput. Syst., vol. 28, no. 6, pp. 833–851, Jun. 2012.

[7] A. R. Javed, R. Abid, B. Aslam, H. A. Khalid, M. Z. Khan, O. H. Alhazmi, and M. Rizwan, "Green5G: Enhancing capacity and coverage in device- to-device communication," Comput., Mater. Continua, vol. 67, no. 2, pp. 1933–1950, 2021.

[8] M. Anuradha, T. Jayasankar, N. B. Prakash, M. Y. Sikkandar, G. R. Hemalakshmi, C. Bharatiraja, and A. S. F. Britto, "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," Microprocessors Microsyst., vol. 80, Feb. 2021, Art. no. 103301.

[9] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, A. K. Bashir, S. Mumtaz, and S. A. Otaibi, "Blockchain-enabled reliable osmotic computing for cloud of things: Applications and challenges," IEEE Internet Things Mag., vol. 3, no. 2, pp. 63–67, Jun. 2020.

[10] R. B. Uriarte and R. DeNicola, "Blockchain-based decentralized cloud/fog solutions: Challenges, opportunities, and standards," IEEE Commun. Standards Mag., vol. 2, no. 3, pp. 22–28, Sep. 2018.



