Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 13, Issue. 9, September 2024, pg.34 – 41

Risks and Challenges of Using Cloud Computing in the Internet of Things

Yassen AbdelKhaleq Najm[1*]

[1]College of Medicine, Al-Iraqia University, Baghdad, Iraq

DOI: https://doi.org/10.47760/ijcsmc.2024.v13i09.005

Abstract: The term Internet of Things (IoT) did not differ from other terms in its origins, as its first signs appeared in the industrial and commercial sectors. Therefore, the benefits of this technology must be generalized to all sectors to achieve intelligent communication resulting from advanced Internet protocols, cloud services, and smart devices such as smartphones. The combination of cloud computing and IoT is associated with more security vulnerabilities. For various reasons, security is seen as the most critical concern when integrating an IoT system with the cloud. This study aimed to identify the risks and challenges of using cloud computing in the Internet of Things. The study followed the descriptive approach to explain the risks and challenges of using cloud computing. The concept of the Internet of Things and cloud computing was explained, and the challenges and risks associated with them. In addition to, the risks resulting from integrating cloud computing into the Internet of Things.
Keywords: Network; Cloud Computing; Cloud Risk; Internet of Things; IoT Security.

1. Introduction

The development of information and communications technologies is currently increasing steadily, and in light of the steady growth of information technology. Internet of Things technology is considered the fourth information revolution after the revolution of computers, the Internet, communication networks, and mobile phones. So, human contact with the device or another device becomes necessary to conduct transactions. Through the Internet of Things technology, there is an exchange of data between individuals, between individuals and things, and between things with each other at any time and in any place, by integrating or installing sensors inside things and connecting them to the Internet, and then these sensors automatically operate the data and connect it to Information users [1]. On the other hand, to keep pace with the rapid development of dealing through Internet networks to transform into the automation of processes. Computing is considered a technology based on storing, processing, and transferring computer data to the so-called cloud over the Internet. So, the programs transform from products to services, which contributes to easy access by users of data via the Internet, and the possibility of updating data in real-time [2]. It is through these New Developments that Smart cities have been created, and restaurants, airports, and commercial and health institutions have been developed. Despite the great opportunities offered by the Internet of Things in general and cloud computing in particular, they also face challenges and risks such as security, privacy, and reliability. It is therefore important to enhance security and privacy and develop new protection technologies. The Internet of Things can be used to improve environmental sustainability, preserve natural resources, and provide effective solutions to current environmental challenges. It is expected that the developments of the Internet of Things and cloud computing will continue in the coming years, making it one of the most important modern and future technologies.

The Internet of Things (IoT) sensors intentionally communicate with other real-world linked things to gather various operational metrics and disseminate the information to other systems and devices [3]. IoT networks become more intelligent and have access to larger data streams and greater IoT connectivity thanks to artificial intelligence (AI) [4]. The enormous amount of data generated by the quick expansion of IoT sensors will require a significant amount of processing and storage space [5].

For data collection, storage, processing, and visualization, there are many popular methods, such as edge device clouds and on-premises private clouds. However, Internet of Things data is sent across the network to distant cloud centers, with public cloud environments emerging as the most efficient and cost-effective choice for large-scale data processing and storing. In the public cloud environment, there are automated systems for data management, observability, analysis, storage, and upkeep. The main shortcomings of IoT, notably low processing power, low computational power, and restricted storage, can be addressed by cloud computing with its quick and flexible resource supply at low cost [6].

Furthermore, cloud computing supports IoT systems by guaranteeing business continuity and supplying sufficient resources. Automation of smart grids, intelligent energy, and intelligent cities are just a few of the beneficial applications that have been developed as a result of IoT and cloud [7].

The combination of cloud computing and IoT is linked to more security vulnerabilities. When an IoT system is integrated with the cloud, security becomes the primary worry for a variety of reasons, including incorrect device updates, a lack of reliable protocols, a lack of device monitoring, a failure to update default passwords, and careless use [8]. Additionally, weak, guessable, and hardcoded passwords make the built-in authentication method of IoT devices unreliable [9].

On this basis, this study came as a theoretical proposal to clarify the risks and challenges of using cloud computing. To achieve this, it is necessary to define the terms cloud computing and the Internet of Things, as well as to list their uses, dangers, and obstacles. The nature of the topic imposed the use of a descriptive approach through readings and an attempt to project it onto the research topic. The importance of the study comes from the importance of the Internet of Things and cloud computing in various areas of life.

2. The Concept and History of the IoT

Kevin Ashton coined the phrase "Internet of Things" in the early 2000s while he was employed by Procter & Gamble to enhance the vocabulary of their distribution system through the Internet's connection of RFID data. In the year 2000, LG announced its plan to display its product, the first refrigerator connected to the Internet. In 2005, the International Telecommunication Union adopted the term Internet of Things (IoT) in its annual report, and in 2008 the IPSO alliance was formed to develop the use of Internet devices and protocols in energy, consumption, health care, and industrial applications. In 2012, the IPV6 protocol was launched, which allows protocols to be defined between each other without restrictions, thus ensuring communication between millions of devices around the world.

Many studies have focused on the term Internet of Things since its emergence and several definitions have emerged. The Internet of Things, it is a system of interconnected devices connected to a network or to each other, where data is exchanged without necessarily requiring human-to-human interaction. Sometimes referred to as "smart devices", IoT devices use software, drivers, and network connections to each other. In other words, IoT is a group of electronic devices that can share information [10]. As defined by [11], it is a network that allows flexibility, visibility, tracking, and information exchange by linking physical objects digitally with sensors, monitoring, and interaction within the facility, in addition to linking the physical objects in the facility to its supply chain, which facilitates control and coordination of all Operations promptly.

Components of the physical architecture of Internet of Things technology [12]:

- Things: Anything that can be connected to the Internet, which may be a living organism such as a human or a non-living component such as (computers, machinery and equipment, smartphones, cars, etc.).
- RFID radio frequency identification technology: It works to identify, track, collect, and transmit information through automatic recognition and tracking of tags attached to objects, by installing a chip called TAG RFID that allows the physical movement of tags to be tracked indirectly in real-time.
- Wireless Sensor Network (WSN): It consists of independent nodes distributed spatially, and a group of sensors to monitor and track the status of various devices such as their location and movements.
- Storage units (cloud): It is an Internet-based computing platform that enables the effective management of a very large group of different computing resources and the storage of data generated from sensors and access to it by the dog.
- Middleware: This is a service-oriented resource package, which is used to connect both sensors and controllers to the cloud.

3. Cloud Computing and its History

The term “cloud computing” was first used by Ramni Chellappa in 1997. It began as a term to describe small networks that can be likened to the Internet in two eras. The use of cloud diagrams to describe services performed by computers in an interconnected network date back to 1977. The first network that used TCP/IP5 protocols (which are the basis for communication in modern networks, including the Internet) to communicate between a group of computers, was called ARPANET [13].

Cloud computing is a term that refers to computer resources and systems that can be rented over the Internet by companies. Cloud computing provides computer services such as servers, storage, databases, networks, software, and business intelligence [13]. The US National Institute of Standards and Technology defines cloud computing as a means of enabling user-perpetual and convenient access to a network depending on the use and sharing of a collection of computer resources (servers, networks, storage, apps, and services) that can be swiftly and easily set up by management or through communication with Supplier of Services [14].

4. Cloud Computing Categories [15]

- Infrastructure as a service (IaaS): It is the basis of cloud computing. It includes storage, backup, databases, and security. It allows the company or user to rent part of the cloud computing servers to a cloud computing service provider and pay according to usage, such as in electricity or water bills.
- Platform as a service (PaaS): The foundation of PAAS is the provision of an environment for software application development, testing, delivery, and management that is available on demand. Its purpose is to simplify the process of developing web or mobile apps by eliminating the need to worry about configuring or maintaining the server, storage, network, and database infrastructure. That is, a company that wants to design websites or applications does not have to rent infrastructure, but only a platform for design, delivery, and testing.

- Software as a service (SaaS): is the most accessible service for users and non-profit organizations, as it allows them to use applications and software and host them to maintain them (update them and improve their gaps) because they are connected to the application infrastructure.
- Function as a service (FaaS): It enables developers to launch, develop, or update a program without consuming infrastructure, that is, without adding costs.

Figure 1 below shows how IaaS, PaaS, SaaS, and FaaS compare in terms of client and service provider responsibilities under different hosting models.

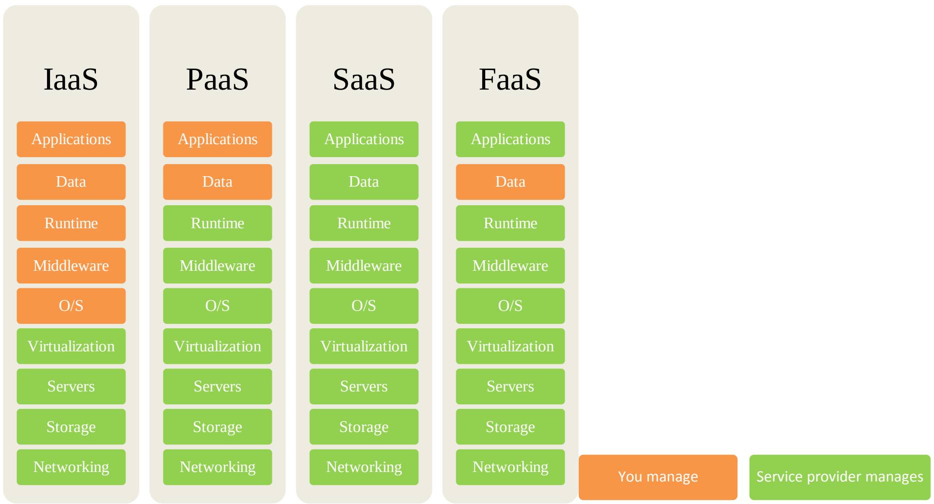

Figure 1. Client and service provider responsibilities under different hosting models.

5. IoT Security

The three main information security concerns are Availability, Integrity, and Confidentiality:

- Confidentiality serves to keep private information from being accessed by unauthorized individuals [16]. Devices of the same type or design are shipped with default passwords in an IoT context. Oftentimes, users fail to update such passwords. Using default passwords leads to vulnerabilities and is risky [17].
- Integrity pertains to guaranteeing the genuineness of information shared by prohibiting any tampering or alteration of the information [16].
- Availability refers to ensuring that the information or systems are always available when requested [16]. According to [18] an IoT device may share information with other devices within the same network if one cannot provide the necessary functionality.

According to [16], the measures taken to maintain information security are:

- An authorization is a type of security measure that aims to ensure that a user has the necessary rights to perform a specific task or operation.
- A security system that grants only authorized individuals' access to certain restricted areas is called access control.
- The authenticity of an individual's identity involves confirming the request against their specific identity documents.
- Non-repudiation involves employing digital signatures and timestamps to establish proof of certain activities so they cannot be later revoked.

- The capacity of several systems to connect, communicate, and share data without hindrances is known as interoperability.

6. Security Risks at Every IoT Layer

According to [19], the main security and attack concerns on the application layer of the Internet of Things include data authentication, data privacy, permission, availability, and confidentiality. The three layers of the Internet are perception, network, and application. According to [20], the main security threats at the network layer are DoS, eavesdropping, and routing attacks. According to [21], the main security threats in the perception layer are DoS attacks and Sybil attacks, among others.

7. Cloud Computing Security Flaws

NIST has defined the essential requirements for cloud security, which include availability, confidentiality, privacy, authorization, and integrity.

The Cloud Security Alliance [22] released a list of the top eleven most significant dangers to cloud computing:

- Confidential or sensitive data breaches happen when someone reads, distributes, or steals information without authorization. It could be the consequence of a mistake, insufficient security, application flaws, or the main objective of a deliberate attack.
- Misconfiguration and Inadequate Change Control: A faulty setup might result in misconfiguration, which exposes the asset to intrusions.
- Absence of a cloud security architecture and strategy: Public cloud computing is starting to replace enterprise infrastructure.
- Inadequate Identity, Credential, Access, and Key Management: These refer to the instruments that a business employs to grant users access to its assets, including servers, files, and computer systems. Events such as weak password usage, inadequate credential management, and non-use of multifactor authentication can result in vulnerabilities and data breaches.
- Account Hijacking: In this scenario, a malevolent actor gains access to sensitive or privileged accounts. These accounts are vulnerable to phishing scams, credential theft, and cloud system exploits.
- Insider Threat: An insider threat is a person or entity that has access to resources and has been authorized to use them but can abuse that access to harm the organization.
- Insecure Interfaces and APIs: To enable customers to engage with and oversee cloud services, providers reveal a series of interfaces and APIs to them. The security of the API may have an impact on cloud security.
- Weak Control Plane: A control plane is perfect for data duplication and storage during a service migration to the cloud. In addition to providing stability throughout runtime, it guarantees security and integrity. A weak control plane means that there are potential blind spots that could lead to data corruption, leakage, or unavailability and that the data isn't entirely under the administrator's control.
- Failures in the Applistructure and Metastructure: These are essential parts of any cloud service. Regular disclosure of security procedures undertaken by providers to safeguard their systems is common. You may think of the metastructure as the demarcation line for the consumer. Choosing how much information the provider must divulge is crucial. Configuration errors can cause disruptions to the cloud and cause financial and operational harm to tenants.
- Limited Cloud Usage Visibility: This happens when a company can't determine if a service that's utilizing its platform is dangerous or safe. There are generally two main categories: authorized app abuse and unauthorized app

use. When consumers utilize apps and services without authorization, the former happens. The latter occurs when authorized users make use of an approved program.

- Misuse and Malicious Utilization of Cloud Services: An attacker may target consumers by utilizing cloud resources.

8. Security Challenges in IoT and Cloud Integration

For the following reasons, security in IoT and cloud integration becomes a key concern.

8.1. Security and Privacy

Data transfer from the real world to the cloud is made possible by the cloud-based Internet of Things. However, this presents a challenge for data privacy protection because data is stored in various countries with varying privacy regulations, and the data will likely be accessed by foreign parties. Thus, it is essential to have the right licensing guidelines and regulations in place while making sure that only authorized individuals have access to sensitive data.

This is especially important when it comes to protecting user privacy, as data integrity needs to be ensured [23]. Furthermore, issues with service level agreements (SLAs), the physical location of the data, and mistrust of the service provider also occur when important Internet of Things applications migrate to the cloud [24]. Strong authentication and permission control are therefore necessary, as they are regarded as the first line of defense against unauthorized actions [25]. Additionally, companies that depend on outside vendors for tools and equipment have little control over security configurations due to a lack of visibility and control. Furthermore, users of the gadgets do not have complete visibility because they are unaware of how the devices operate internally. Hackers can obtain illegal access with the aid of elevated user permissions, weak default user passwords, and insufficient access control [26].

8.2. Heterogeneity

The broad heterogeneity of current devices, platforms, operating systems, and services that can be employed for new or upgraded applications is a significant hurdle for cloud-based IoT approaches. Cloud platforms have problems with heterogeneity. Furthermore, end users adopting several cloud techniques might make the heterogeneity challenge worse, as services will need to rely on multiple service providers to enhance application resilience and performance; IoT gadgets impose processing power limits, and public key cryptography cannot be extended to all layers due to these factors in addition to the unique security aspects of each type of device [23]. It becomes challenging to deploy uniform security across heterogeneous devices as a result. a rise in security vulnerabilities as a result of interoperability problems brought on by disparate communication protocols and standards between devices [27].

8.3. Big Data

IoT data may be more easily stored on cloud platforms and can be subjected to sophisticated analysis. The speed of the entire program is highly dependent on the features of this data management service, therefore handling the massive volume of data generated is a critical issue. It's still quite difficult to find the perfect data management solution that enables cloud computing to handle enormous volumes of data. Furthermore, data integrity is essential due to security and privacy concerns, the majority of which are connected to external data, as well as its effect on quality of service (QoS) [23].

Large amounts of bandwidth are needed to transfer the massive amounts of data produced by Internet-connected devices to the cloud. This is because broadband growth is not keeping up with the advancements in computing and storage [23]. Consequently, the primary challenge lies in obtaining sufficient network performance to transfer data to cloud environments. The cloud-based IoT model allows for the creation of new applications targeted at integrating and analyzing real-world data into IoT objects. According to [28], this calls for interaction with billions of devices spread across numerous locations, where Internet of Things devices must deal with latency dynamics and connectivity problems [23].

9. Conclusion

The Internet of Things (IoT) is expanding due to the sharp increase in the number of devices linked to the Internet. Cloud computing has become an essential part of the Internet of Things ecosystem because it offers resources for storing IoT data, helps with data processing, and supports visualization and actions. Threats to the security of both cloud and IoT technologies increase with their combination. Security flaws can jeopardize an IoT system, and vice versa. This paper reviews the risks resulting from cloud computing in the Internet of Things, as the study showed the security risks represented by privacy, large data, and heterogeneity that must be resolved for cloud computing to be effective in the Internet of Things. Future studies need to study ways to address the problems resulting from integrating cloud computing into the Internet of Things.

Acknowledgements

The authors would like to thank Al-Iraqia University for its academic guidance and assistance. (https://aliraqia.edu.iq),

References

[1]. R. M. Mashat, S. H. Abourokbah, and M. A. Salam, "Impact of Internet of Things Adoption on Organizational Performance: A Mediating Analysis of Supply Chain Integration, Performance, and Competitive Advantage," *Sustainability*, vol. 16, no. 6, p. 2250, Mar. 2024, doi: 10.3390/su16062250.

[2]. M. Giannakis, K. Spanaki, and R. Dubey, "A cloud-based supply chain management system: effects on supply chain responsiveness," *Journal of Enterprise Information Management*, vol. 32, no. 4, pp. 585–607, Jun. 2019, doi: 10.1108/JEIM-05-2018-0106.

[3]. A. M. Herrera *et al.*, "Effective Use of Embedded Platforms in the Development of Experiments for Enhancing the Interests of STEAM Students in Mexico," 2023, pp. 130–146. doi: 10.4018/978-1-6684-5920-1.ch007.

[4]. S. Khanam, S. Tanweer, and S. S. Khalid, "Future of Internet of Things: Enhancing Cloud-Based IoT Using Artificial Intelligence," *International Journal of Cloud Applications and Computing*, vol. 12, no. 1, 2022, doi: 10.4018/IJCAC.297094.

[5]. S. Qabil, U. Waheed, S. M. Awan, Y. Mansoor, and M. A. Khan, "A Survey on Emerging Integration of Cloud Computing and Internet of Things," in *2019 International Conference on Information Science and Communication Technology (ICISCT)*, 2019, pp. 1–7. doi: 10.1109/CISCT.2019.8777438.

[6]. 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 *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, Institute of Electrical and Electronics Engineers Inc., Jul. 2017, pp. 670–675. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105.

[7]. H. Tian, W. Ye, J. Wang, H. Quan, and C. C. Chang, "Certificateless Public Auditing for Cloud-Based Medical Data in Healthcare Industry 4.0," *International Journal of Intelligent Systems*, vol. 2023, 2023, doi: 10.1155/2023/3375823.

[8]. L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Applied Sciences (Switzerland)*, vol. 10, no. 12, Jun. 2020, doi: 10.3390/APP10124102.

[9]. N. Sivaselvan, K. V. Bhat, M. Rajarajan, A. K. Das, and J. J. P. C. Rodrigues, "SUACC-IoT: secure unified authentication and access control system based on capability for IoT," *Cluster Comput*, vol. 26, no. 4, pp. 2409–2428, Aug. 2023, doi: 10.1007/s10586-022-03733-w.

[10]. S. Hinson and N. Sutherland, "DEBATE PACK Regulating the Internet of Things," 2019. [Online]. Available: www.parliament.uk/commons-library|intranet.parliament.uk/commons-library|papers@parliament.uk|@commonslibrary

[11]. M. Ben-Daya, E. Hassini, and Z. Bahroun, "Internet of things and supply chain management: a literature review," *International Journal of Production Research*, vol. 57, no. 15–16. Taylor and Francis Ltd., pp. 4719–4742, 2019. doi: 10.1080/00207543.2017.1402140.

[12]. Y. Mao and L. Zhang, "Design and Implementation of Port Bulk Storage Management System Based on Internet of Things Technology," *J Coast Res*, vol. 98, no. sp1, pp. 62 – 66, 2019, doi: 10.2112/SI98-016.1.

[13]. R. Nazir, Z. Ahmed, Z. Ahmad, N. Shaikh, A. Laghari, and K. Kumar, "Cloud Computing Applications: A Review," *EAI Endorsed Transactions on Cloud Systems*, vol. 6, no. 17, p. 164667, May 2020, doi: 10.4108/eai.22-5-2020.164667.

[14]. P. M. Mell and T. Grance, "The NIST definition of cloud computing," Gaithersburg, MD, 2011. doi: 10.6028/NIST.SP.800-145.

[15]. K. Kaur, "A Review of Cloud Computing Service Models," 2016.

[16]. Imran, S. M. Ali, M. M. Alam, and M. M. Su'ud, "A Survey of IoT Security Issues - From Past to Future Trends," *Journal of Computer Science*, vol. 17, no. 11, pp. 1038–1045, 2021, doi: 10.3844/JCSSP.2021.1031.1045.

[17]. J. Sen, "Security and privacy issues in cloud computing," in *Standards and Standardization: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2015, pp. 1370–1414. doi: 10.4018/978-1-4666-8111-8.ch065.

[18]. M. Trnka and T. Cerny, "Authentication and Authorization Rules Sharing for Internet of Things," *Software Networking*, vol. 2017, no. 1, pp. 35–52, 2016, doi: 10.13052/jsn2445-9739.2017.003.

[19]. E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Trans Industr Inform*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

[20]. K. Chen *et al.*, "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," *Journal of Hardware and Systems Security*, vol. 2, no. 2, pp. 97–110, Jun. 2018, doi: 10.1007/s41635-017-0029-7.

[21]. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Security and Communication Networks*, vol. 2018. Hindawi Limited, 2018. doi: 10.1155/2018/5978636.

[22]. A. Sen and S. Madria, "Data analysis of cloud security alliance's security, trust & assurance registry," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jan. 2018. doi: 10.1145/3154273.3154343.

[23]. T. Alam, "Cloud-based iot applications and their roles in smart cities," *Smart Cities*, vol. 4, no. 3. MDPI, pp. 1196–1219, Sep. 01, 2021. doi: 10.3390/smartcities4030064.

[24]. A. Alenezi, N. H. N. Zulkipli, H. F. Atlam, R. J. Walters, and G. B. Wills, "The impact of cloud forensic readiness on security," in *CLOSER 2017 - Proceedings of the 7th International Conference on Cloud Computing and Services Science*, SciTePress, 2017, pp. 511–517. doi: 10.5220/0006332705390545.

[25]. G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Trust Management in Decentralized IoT Access Control System," Dec. 2019, [Online]. Available: http://arxiv.org/abs/1912.10247

[26]. N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.

[27]. P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, "Internet of Things: Security and Solutions Survey," *Sensors*, vol. 22, no. 19. MDPI, Oct. 01, 2022. doi: 10.3390/s22197433.

[28]. C. Surianarayanan and P. R. Chelliah, "Integration of the Internet of Things and Cloud: Security Challenges and Solutions - A Review," *International Journal of Cloud Applications and Computing*, vol. 13, no. 1. IGI Global, 2023. doi: 10.4018/IJCAC.325624.