Pakistan Journal of Engineering and Technology
ISSN (Print): 2664-2042; ISSN (Online): 2664-2050
Received: 2023-06-11
Accepted: 2024-01-05
https://doi.org/10.51846/vol6iss4pp1-6

PAKJET
Pakistan Journal of Engineering & Technology

Review

A Review about Internet of Things (IoT) Integration with Cloud Computing with a Limelight on Security

Umm e Kulsoom [1], Syeda Faiza Nasim [2,*], Asma Qaiser [1], Sidra Aziz [3], and Syeda Alishba Fatima [2]

[1] Department of Computer Science, Iqra University, Karachi, Pakistan
[2] Department of Computer Science and Information Technology, NED University of Engineering & Technology, Karachi, Pakistan
[3] Aligarh Institute of Technology, Karachi, Pakistan
* Correspondence: Syeda Faiza Nasim (sfaizaadnan@gmail.com or sfnasim@cloud.neduet.edu.pk)

Abstract: Cloud computing has become a pivotal and widely embraced technology due to its accessibility and cost-effectiveness. This review explores the intersection of cloud computing and Internet-of-Things (IoT) devices, highlighting the remarkable advancements made in resource utilization and storage methods. However, this rapid growth has also raised concerns about security. Through an in-depth analysis of recent research, we examine the security challenges associated with IoT-based cloud computing, including account hacking, phishing, malware, middleman attacks, and service denial. We also discuss the potential benefits, architectural integration options, and the impact of IoT on cloud computing. This review paper categorizes findings and solutions from recent research papers, ultimately shedding light on the vulnerabilities and weaknesses of IoT-based cloud computing, along with its performance and stability issues.

Keywords: Cloud Computing, IoT, IoT Security, Cyber Security, Cloud Attacks, Cloud Attacks Prevention

1. Introduction

1.1. Background and Motivation

The topic of cloud based IoT has many dimensions. It is basically a framework that allows and assists the user with servers, storage, data, securing your data, and many more resources, which could've been difficult to tackle if there was no such framework like Internet of Things based cloud computing [1]. Cloud computing grants the user access to and keeps you up to date about the components of your system (e.g., software, hardware), no matter if your system is on an industrial level. Users can also enjoy skillful and competent usage of the network, which also provides vast options to secure their interests [2]. Cloud Computing is a word that is used more often nowadays and helps the industry with large number of options in servers, security, storage, platforms, and much more. The prosperity and eminence of cloud computing are heavily dependent on giving the finest knowledge and involvement to cloud administrators, software developers, and users in the end. But everything has its pros and cons; there are some cons to the usage of cloud computing in terms of acceptance, security, control, cost, etc. The main focus, which is severe, is on security, as there could be more than one layer of data and applications with respect to the selected cloud service model. Faith and confidence are also concerns, as they are precisely interlinked with the authority of the providers of cloud services. As data is stored using traditional techniques, it also experiences attacks. IoT is an infrastructure that is progressing at a very high speed in this time of the world. As IoT is playing its part in many ways in our lives, its users are increasing exponentially. In this decade and the last decade, the IoT has been deployed in many ways in our daily lives, such as in the health sector [3, 4], smart homes [5], systems, and cities [6]. Nonetheless, IoT is not capable of handling and entertaining a large number of users and their requirements; however, integration with cloud computing of IoT can be helpful. IoT is still struggling with its issues, with most of the focus on security, which, if not handled properly, can disturb the whole architecture of IoT. The combination of cloud computing and IoT has progressed and emerged as the most futuristic and advanced technology. Nowadays, the speed with which it is growing is unbelievably fast. The integration of these two can result in powerful and productive usage and management of resources. This paper looks into the security challenges that lie under the umbrella of Security in IoT-based cloud computing [7, 8, 9, 10].

1.2. Literature Review

This section of the research paper examines and questions the information learned from reading the research papers on IoT-based cloud computing. With regard to IoT-based cloud computing, the examination is mostly focused on the security issue and its solution. There are many risks involved when it comes to security in IoT-based Cloud Computing. Loss of Data is one of the severe issues that have been questioned hugely. It also has significant importance to any organization or company. The data is always at great risk if the safety techniques are not executed perfectly. A lot of improvement is required to enhance security techniques by looking at this issue closely so that the data loss will be reduced to some

extent [11]. The factors that are concerned with security concerning personal data, i.e., the advancement and enhancement of techniques and technologies that are meant to be used for privacy and relevant issues. The other motive is to develop ideal software that can administer and take care of the identities of objects and users [12, 13]. Hacking and stealing data is also a point of concern. SQL injection is a highly common attack in data breaches [14, 15].

Other security threats that are affecting the progression of IoT-based Cloud Computing are breaching of data, insecurity of Application Programming Interface (API), underprivileged architecture and techniques, broken management, hijacking and corrupting of accounts, usage of cloud transparency [15], and many more, which will be discussed ahead. The security threat also includes cybersecurity threats. The common and popular threats to cyber security involve no legal connection, leaking of information, baseless data, inoperative facts and information, traffic inquiries, and unofficial and nonidentity access [16]. Cybersecurity is also a very common area of interest in the field of computer science, which is attracting more talented and useful individuals to help eliminate or reduce these threats. It is very important to achieve the most high-end possibilities for security and to accomplish that, the data security needs and regulations should be clarified properly before integrating it with the cloud [17, 18]. In [19], the authors described a data security flaw in cloud computing that occurs when a guest OS is run over a hypervisor without knowledge of the guest OS's dependability. The authors of [20] presented a survey that categorized the most recent techniques for data replication schemes along with any unresolved problems. According to recent research, when the cloud is used for various data storage purposes, it exposes users' sensitive information while also enabling network-based access to communication tools like emails and calendars, use of other tools, such as Microsoft Office and Google Docs, through the internet for application development, testing, and business use, as well as data backup and restoration. Security and privacy are, therefore, extremely important. The cloud is utilized by a user for a variety of reasons. Data is endlessly stored away from the machine that the data owner controls. How the information is used and stored are two domains where the data owner lacks expertise [21].

The function of a virus that attacks an economic system's financial documents or disrupts a nation's stock market, or by sending an incorrect message, causing the nation's power plant to stop and fail, or even by disrupting the air traffic control system, resulting in air accidents, are just a few examples of scenarios for severe and occasionally widespread physical or economic harm [22].

Reference [23] provides a security system based on digital signatures that provides authentication, data integrity, and defense against cyberattacks. The findings of this study demonstrate that the Semiconductor Equipment Communication Standard/Generic Equipment Model (SECS/GEM) is a reliable communications system for securing industrial equipment from communication with unauthorized parties. Additionally, SECS/GEM communications showed that they could defend industrial equipment against replay, denial-of-service, and fake data injection attacks. The data collected by the sensors in healthcare wearable devices (HWDs) may be distorted and noisy because the majority of wearables contact the epidermis. Body hair on the skin that causes less adhesion between the skin and the garment and continual body motion are two causes of the noise. Since HWDs have been found to have many uses for monitoring, additional work needs to be done to adapt them for use in diagnostic procedures. This is due to HWDs' inadequate integration with the majority of diagnostic procedures, which rely on samples like blood, urine, and saliva. As a result, further work must be done to integrate HWDs with platforms that can support the usage of biological samples with HWDs and can be used by the end user, which, therefore, requires more work. Additionally, the application of AI algorithms, such as the supervised learning regression algorithm, can be utilized to monitor the behavior of numerous prognostic factors [24].

Protection of the wearer's privacy must not be compromised because HWDs include protected health information (PHI). Secure communication protocols in HWDs are crucial for this reason in order to protect wearers' privacy and security [25], [26], [27].

There are many types of security threats, but most of the security concerns are at the network level, general security level, and application level. Every threat has many types, which help to precisely find the solution to that particular threat. All the types will be discussed ahead of time in this paper.

2. Materials and Methods

Our research survey is based on the most recent and sophisticated studies on the topic of interest. To ensure the relevance and endurance of our review paper process. Specifically,

- Time Frame Selection: We focused on research articles published between 2019 and 2022 to guarantee that our review remains current and relevant in the next few years.
- Scope Refinement: We excluded surveys and research that were unrelated to IoT and Cloud Computing. This conscious option was made to streamline our paper, minimizing diversity and complexity.
- Precise Focus: Our survey is particularly concerned with investigating the security elements of IoT-based Cloud Computing, ensuring a concentrated and in-depth examination of this vital subject.
- Avoiding Repetition: In order to improve the clarity and readability of our evaluation, we have made every effort to avoid repetition and verbosity.

By adhering to these standards, we produce a comprehensive and brief review paper that provides significant insights into the security problems of IoT-based cloud computing, which are:

2.1. Threats to IoT-Based Cloud Computing Security:

Cloud computing's increasing growth in numerous industries has made it an appealing target for cyber attackers. Cloud services are the backbone of modern enterprises, storing crucial data, apps, and resources. As a result of the possibility of large benefits, bad actors have increasingly moved their focus to cloud computing [8]. This trend is especially concerning for Internet of Things (IoT) integration, where cloud infrastructure credibility is critical.

2.1.1. Account Hijacking and Hacking in IoT Cloud Environments:

Unauthorized access to and takeover of user accounts is one of the most common security issues in IoT-based cloud computing. In these attacks, infiltrators use a variety of illegal tactics to breach user accounts within the cloud ecosystem. The primary goal is to steal important organizational resources, sensitive data, and other assets from these accounts, frequently with the idea of misusing them or launching large-scale attacks in the future. Such violations can have serious implications, including money losses, client relationship damage, and reputational injury. Notably, the frequency of these attacks has increased dramatically in recent years, causing many firms to form specialized cybersecurity teams and implement strong security measures [28].

2.1.2. Phishing Schemes:

Phishing attacks are a prevalent tactic used by cybercriminals to obtain unauthorized access to user accounts. Malicious actors often send false emails, messages, or documents that appear authentic and solicit victims to provide their login credentials in a phishing assault. Once these credentials are provided, the attackers can breach the victim's account. To protect against phishing attacks, it is critical to thoroughly examine email sources, particularly those from dubious senders. Always double-check links before clicking on them, and keep personal and commercial information separate. Block and report any suspicious behavior as soon as possible.

2.1.3. Malware Attacks:

Malware assaults use harmful software to infiltrate cloud settings. The strategies used differ depending on the cloud architecture. Attackers intend to insert malicious programs or services into the cloud and authenticate them in order to obtain access. They then use these applications to penetrate the cloud, possibly jeopardizing an organization's sensitive data and resources. Notably, IoT devices are especially vulnerable to malware attacks, with the Mirai malware serving as a prime example.

2.1.4. Port Attacks:

Port-based attacks target specific ports used by a company's services. Such attacks offer a substantial risk, capable of undermining an organization's integrity and threatening the privacy of its cloud resources. To effectively counter port-based attacks, businesses must obtain synchronized threat intelligence on a proactive basis. Furthermore, it is critical to employ specialized security software capable of screening for these risks before they progress beyond recovery.

- **Middle Man Attacks:** Middle-man attacks occur when malicious actors intercept and manipulate communications between two parties, frequently resulting in the leak of extremely sensitive information. Detecting and identifying the attacker can be a difficult task. The most successful strategy for preventing Middle Man Attacks is to deploy robust security measures such as message encryption techniques and the use of Virtual Private Networks (VPNs) or isolated Wi-Fi networks.
- **Botnet Attacks:** Botnet attacks employ hacked device networks to circumvent contemporary cloud computing security and execute malicious actions on a user's network resources. Because of their quick deployment and smooth operation, these attacks are difficult to identify and mitigate. Maintaining up-to-date software, monitoring and reporting failed login attempts, and establishing stringent network security protocols are all effective defenses.

2.1.5. Service Denial Attack:

Service Denial Attacks are designed to disrupt cloud services by preventing customers from accessing their data, photos, and resources. Sluggish system performance and degraded cloud functioning are indicators of such attacks. Multiple attackers can coordinate these attacks at the same time, a technique known as Distributed Denial of Service (DDoS).

2.2. Security Issues in IoT-Based Cloud Computing:

There are significant security issues in IoT-based Cloud Computing, including data security, service security, and resource security.

2.2.1. Data Security:

Data security is crucial in IoT-based Cloud Computing because failure to do so might result in the loss or leakage of critical organizational data. Data transmission from nimble IoT devices to the Cloud is frequently done via wireless networks, which increases the danger of illegal access and data manipulation. While IoT-based Clouds provide limited user data optimization and access via virtual machines, revoked access privileges can expose vulnerable users to abuse. Another key problem is hiding data locations, with user data kept across multiple unreported cloud columns and stages. This lack of transparency raises security concerns despite the fact that tracking data is difficult but not impossible. Furthermore, in order to avoid costly service installations, cloud providers frequently replicate data across multiple geographical locations, thus widening the attack surface.

2.2.2. Network Level Security:

Network security entails protecting public, private, and shared networks from threats. It is critical to put strong protective procedures in place. Domain Name Server (DNS) attacks are a prevalent danger that aims to prevent diversion to unauthorized servers. DNS security, on the other hand, may not be perfect, especially when IP addresses are reused [13]. Furthermore, network-level assaults such as Sniffer attacks arise when unencrypted data packets traverse the network. Address Resolution Protocols (ARP) and Round Trip Time (RTT) detection technologies are used to combat these threats.

2.2.3. Application Level Security:

Application-level security ensures that only authorized users have access to a system's software and hardware. Attackers frequently try to impersonate authorized users in order to gain unauthorized access for malevolent reasons [11]. These attacks arise when the network layer fails to recognize legitimate users, necessitating the implementation of advanced security measures to prevent them. Some typical application-level dangers include "Cookie Poisoning," in which attackers attempt to modify information saved in cookies in order to gain unwanted access, which can be avoided by regular cache clearing. Another concern is hidden fields on websites, which are normally accessible exclusively to site owners and developers. Attackers target these places in order to change website data and resources without being detected [13].

2.3. Security Solutions in IoT-Based Cloud Computing:

This section describes current security solutions for dealing with security issues in IoT-based cloud computing. In the field of network security, enterprises typically use intrusion detection in cloud IoT, specialized software for identifying network security vulnerabilities in IoT Cloud environments, IoT, and cloud integration to provide safe connections for lightweight devices. For data security, enterprises construct safe environments for multi-cloud data sharing and use coordinated encryption approaches, frequently employing cloud computing frameworks such as Hadoop [17]. Encryption is used in privacy solutions to check data authenticity using cryptography, allowing for the secure processing of encrypted data. Identification is a vital security feature that enables authorized workers access to cloud resources, lowering the danger of illegal access. Compositions of security controls, rules, and Standards are critical to lowering security threats and leading enterprises in risk reduction. Blockchain technology has developed as a popular security solution in IoT and Cloud Computing, offering high-level data protection. Immutable data storage methods, such as Till Data [18], improve data and resource security by reducing centralized entity control. Anonymization prevents personally identifiable data from being communicated to cloud providers during data transfers. Data segmentation improves security by keeping data segments in independent bits to protect against data association attacks [12]. The problem statements and theoretical solutions regarding cyber security in IoT-based cloud computing are presented in Table 1.

Table 1. Titles, problem statements, and theoretical solutions.

Title	Problem Statement	Theoretical Solution
Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey	With the rapid growth of cloud computing among the industries Questioned the level of security	In accordance with the survey carried out, the solution for the security concerns raised mainly includes software-based assistance to sense the attack and other advanced solutions
The Security Issue in IoT-Cloud: A Review [9]	The immense growth and adoption of IoT technologies are challenged by resource-constrained IoT devices. However, the growth of IoT technologies can be enhanced by integrating them with cloud computing.	Despite the existence of some security solutions in the literature, there are still some open issues that need to be addressed by the experts for security concerns.
A Secure Authentication and Key Agreement Scheme for IoT-Based Cloud Computing Environment [10]	People and organizations can easily accept and apply the services of IoT integrated with. But with the exponential growth of this technology, it has become my favorite target.	To overcome the issues caused by network attacks, an improved authenticated research study for an IoT-based cloud computing environment was introduced.
The Security Challenges in Cloud IoT [11]	IoT and cloud computing, when integrated, offer many facilities to the consumers, like smart devices, etc. A few new kinds of privacy and safety-related problems are introduced.	The new paradigm of cloud computing contains totally new challenges, whole different applications, and a system providing effective usability.

In IoT-based Cloud Computing, security and privacy are paramount. Effective security measures should not only detect but also predict and prevent threats. Table 2 presents an overview of research paradigms, methodologies, algorithms, contexts, and selected research publications to aid in making educated decisions about security approaches.

Table 2. Paradigm/method, algorithm, context /setting /sample.

Paradigm/Method, Algorithm	Context/ Setting/ Sample
The papers used for the assistance of the paper are the latest between the time span of the last 3 - 4 years, and research papers outside the umbrella of IoT and Cloud Computing is excluded [8].	Most of the organizations/companies are using cloud computing as their main service to store their data, resources, etc. It is cost as well as time-efficient

Table 3. Finding/ performance tools and weaknesses.

Finding/Performance Tools	Weaknesses
In this paper, it is tried to find the best solutions regarding the security issues under the umbrella of cloud computing and IoT [8].	Understanding the security requirements and issues first before solving a particular problem. Propose logical ways to reduce the risk of security. Also, prepare for the algorithms that can be used to detect an attack before it is deployed on the system [8]
The problems have been interrogated here the customer of the cloud service provider is facing issues during the connectivity of smart devices [9]	N/A
It mainly focuses on more opportunities and benefits that Cloud IoT can further produce [10].	The cost matter is totally ignored in this paper; no cost efficiency and scales have been measured [10].
In accordance with the old scheme, a number of vulnerabilities were discovered when compared with the proposed adversary model [11]	N/A
IoT is focused on large amounts of data processing in order to provide safe and secure service. IoT is not only composed of physical components but it contains embedded software, sensors and electronics as well [12].	A focus on confidentiality problems and the solutions that can be helpful are proposed [12].
The whole list of security threats in big data computing in accordance with the various layers of the system are identified [13].	A mechanism based on protection of various computing technologies should be identified and analyzed [13].
Since integrated privacy of two significant techs is of higher importance, better solutions are needed for a better future [14].	N/A
It has been deeply noticed that intruders and hackers benefit from glitches in security solutions and poor implementation of security policies i.e. weak passwords, open ports, and unencrypted data [15].	Data security in the cloud is dependent o the safety of data that leads to winning customer's trust in CSP. No theoretical solution provided [15]
The standardization plays a smart role in the IoT security model. Just like the computing technology is slowly moving closer to process information [16]	N/A

3. Results and Discussion

Precisely, the result concluded from reviewing the research papers under the umbrella of IoT and cloud computing is that computing is IoT. cloud Cloud computing integration is a beneficial technology, but the security concerns along with privacy poor stability, are the reason why this technology is not emerging and gaining the attention and acknowledgment it deserves. Although many security solutions are presented to aid this issue, those are not able to achieve the highest of benefits. In Table 3, we have discussed the research papers' findings, performance tools, and weaknesses for the reader to get a clear understanding of what has been discussed and to make comparisons that will make it easier for them to choose the best way to proceed.

By examining the challenges of security and the different solutions that have been demonstrated in this paper, it has been noticed that Cloud Computing security challenges individually make it possible to handle the current security techniques; the same goes for security issues. IoT, but when these two technologies are integrated, no doubt they benefit exponentially, but the security technique on the same page is hard to tackle.

4. Conclusion

The increasing number of users in the field of IoT-based cloud computing is hidden from none. This technology is very beneficial for the Analytics of data providers of data, Wireless and remote service suppliers, mobile phone framework suppliers, and many more people/organizations that work in the field of IoT and Cloud Computing. But no matter how advanced and smart a service is if its security is not up to date and the consumer is not able to trust the service when he stores data and resources, it cannot gain the reputation it deserves. The awareness is phenomenal in this aspect and most organizations and consumers take this security issue very seriously but still, some organizations which are on a small scale do not realize how stringent this issue is and can cost their whole company integrity and reputation. As discussed above, there are several ways to avoid and reduce the risk of security issues, and they are significantly helpful, although there is still so much room left for the upgrading and enhancement of security techniques, policies, and standards, and this room should be filled by the experts as soon as possible to enjoy the advantages of Internet of Things (IoT) based Cloud Computing.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] H. Takabi, J. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24–31, Nov. 2010, doi: 10.1109/msp.2010.186.

[2] C. Stergiou, E. Bompoli, and K. E. Psannis, "Security and privacy issues in IoT-Based big data cloud systems in a digital twin scenario," Applied Sciences, vol. 13, no. 2, p. 758, Jan. 2023,doi: 10.3390/app13020758.

[3] Z. Alansari, S. Soomro, M. R. Belgaum, and S. Shamshirband, "The rise of Internet of Things (IoT) in big healthcare data: Review and open research issues," in Advances in intelligent systems and computing, 2017, pp. 675–685. doi: 10.1007/978-981-10-6875-1_66.

[4] A. Belfiore, C. Cuccurullo, and M. Aria, "IoT in healthcare: A scientometric analysis," Technological Forecasting and Social Change, vol. 184, p. 122001, Nov. 2022, doi: 10.1016/j.techfore.2022.122001.

[5] L. Babangida, T. Perumal, N. Mustapha, and R. Yaakob, "Internet of Things (IoT)-based activity recognition strategies in smart Homes: a review," IEEE Sensors Journal, vol. 22, no. 9, pp. 8327–8336, May 2022, doi: 10.1109/jsen.2022.3161797.

[6] E. F. I. Raj, M. Appadurai, S. Darwin, and E. F. I. Rani, "Internet of Things (IoT) for sustainable smart cities," in CRC Press eBooks, 2022, pp. 163–188. doi: 10.1201/9781003219620-9.
[7] M. Vashishtha et al., "Security and detection mechanism in IoT-based cloud computing using hybrid approach," International Journal of Internet Technology and Secured Transactions, vol. 11, no. 5/6, p. 436, Jan. 2021, doi: 10.1504/ijitst.2021.117414.
[8] 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, doi: 10.3390/electronics11010016.
[9] N. Almolhis, A. M. Alashjaee, S. Duraibi, A. Fahad, and A. N. Moussa, "The Security Issues in IoT - Cloud: A Review," Ieee, Feb. 2020, doi: 10.1109/cspa48992.2020.9068693.
[10] N. Almolhis, A. M. Alashjaee, S. Duraibi, A. Fahad, and A. N. Moussa, "The Security Issues in IoT - Cloud: A Review," Ieee, Feb. 2020, doi: 10.1109/cspa48992.2020.9068693.
[11] S. S. E. Guerbouj, H. Gharsellaoui, and S. Bouamama, "A comprehensive survey on privacy and security issues in cloud computing, internet of things and cloud of Things," International Journal of Service Science, Management, Engineering, and Technology, vol. 10, no. 3, pp. 32–44, Jul. 2019, doi: 10.4018/ijssmet.2019070103.
[12] S. Ray, K. N. Mishra, and S. Dutta, "Big Data Security Issues from the Perspectiveof IoT and Cloud Computing: AReview," Recent Advances in Computer Science and Communications, vol. 14, no.7,pp. 2057–2078, Oct. 2021,doi: 10.2174/2666255813666200224092717.
[13] R. Geetha, A. K. Suntheya, and G. U. Srikanth, "Cloud Integrated IoT enabled Sensor Network Security: research issues and solutions," Wireless Personal Communications, vol. 113, no. 2, pp. 747–771, Apr. 2020, doi: 10.1007/s11277-020-07251-z.
[14] Y. Yu, H. Liang, and J. Chu, "A secure authentication and key agreement scheme for IoT-Based cloud computing environment," Symmetry, vol. 12, no. 1, p. 150, Jan. 2020, doi: 10.3390/sym12010150.
[15] D. K. Saini, K. Kumar, and P. Gupta, "Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions," Security and Communication Networks, vol. 2022, pp. 1–9, Apr. 2022, doi: 10.1155/2022/4943225.
[16] J. Zhang, H. Chen, L. Gong, J. Cao, and Z. Gu, "The Current Research of IoT Security," Ieee, Jun. 2019, doi: 10.1109/dsc.2019.00059.
[17] K. Kambatla, G. Kollias, V. Kumar, and A. Grama, "Trends in big data analytics," Journal of Parallel and Distributed Computing, vol. 74, no. 7, pp. 2561–2573, Jul. 2014, doi: 10.1016/j.jpdc.2014.01.003
[18] S. S. Gill et al., "Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges," Internet of Things, vol. 8, p. 100118, Dec. 2019, doi: 10.1016/j.iot.2019.100118.
[19] S. K. Sood, "A combined approach to ensure data security in cloud computing," Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831–1838, Nov. 2012, doi: 10.1016/j.jnca.2012.07.007.
[20] A. Shakarami, M. Ghobaei-Arani, A. Shahidinejad, M. Masdari, and H. Shakarami, "Data replication schemes in cloud computing: a survey," Cluster Computing, vol. 24, no. 3, pp. 2545–2579, Apr. 2021, doi: 10.1007/s10586-021-03283-7
[21] R. Choubey, R. S. Dubey, and J. Bhattacharjee, "A survey on cloud computing security, challenges and threats," International Journal on Computer Science and Engineering, vol. 3, no. 3, pp. 1227–1231, Mar. 2011,[Online].Available: https://doaj.org/article/a7a09b6e529e45919f8e316c633beb50
[22] M. Snehi and A. Bhandari, "Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks," Computer Science Review, vol. 40, p. 100371, May 2021, doi: 10.1016/j.cosrev.2021.100371.
[23] S.-U.-A. Laghari, S. Manickam, A. Al-Ani, S. U. Rehman, and S. Karuppayah, "SECS/GEMSEC: A Mechanism for Detection and Prevention of Cyber-Attacks on SECS/GEM Communications in Industry 4.0 landscape," IEEE Access, vol. 9, pp. 154380–154394, Jan. 2021, doi: 10.1109/access.2021.3127515.
[24] B. Mohanta, P. Das, and S. Patnaik, "Healthcare 5.0: A Paradigm Shift in Digital Healthcare System Using Artificial Intelligence, IOT and 5G Communication," Ieee, May 2019, doi: 10.1109/icaml48257.2019.00044.
[25] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and Security: challenges and solutions," Applied Sciences, vol. 10, no. 12, p. 4102, Jun. 2020, doi: 10.3390/app10124102.
[26] R. Alharbi and H. Almagwashi, "The Privacy Requirments for Wearable IoT Devices in Healthcare Domain," Ieee, Aug. 2019, doi: 10.1109/ficloudw.2019.00017.
[27] A handbook of internet of things in biomedical and cyber physical system. 2020. doi: 10.1007/978-3-030-23983-1.
[28] Bitdefender. (2023). IoT Security Landscape Report [https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf].