A COMPREHENSIVE ANALYSIS OF CYBERSECURITY IN IOT-BASED CLOUD COMPUTING

Ms. Reena Bhati, Ms.Vaishnavi Pandit, Faculty, Dept. of Computer Science Tilak Maharashtra Vidyapeeth, Pune-37

Abstract

Cloud computing offers a flexible architecture that allows for the dissemination of data and resources across several locations, hence easing accessibility from various industrial settings. As a direct consequence of the proliferation of cloud computing, the industrial sector has seen significant shifts in the utilisation, retention, and distribution of resources, such as data, services, and applications. These changes have been brought about by the cloud. In the business world during the last several years, there has been a considerable growth in the number of companies that employ cloud computing. This trend may be attributed to the desire to capitalise on improved operational efficiency, cost reduction, and increased availability. Furthermore, the integration of cloud computing has played a pivotal role in enhancing the functionality and performance of the internet of things (IoT). Nevertheless, the rapid transition to cloud computing has raised several security issues and presented other obstacles. Cloud-based systems can provide unique challenges when it comes to applying traditional security measures, which might occasionally prove to be insufficient in ensuring effective protection. In recent years, there has been a proliferation of various cyber weapons, leading to concerns over the security and reliability of cloud platforms. However, it is worth noting that significant progress has been made in addressing these problems and mitigating security risks associated with cloud platforms during the last three years. Deep learning, which is a subfield of artificial intelligence, has been making fast strides in recent years, which has resulted in a number of benefits that may or may not be able to give answers to issues about cloud-based industrial security. The following are some of the effects that may be expected from the research that was proposed: The purpose of this article is to provide a comprehensive examination of the architecture, functionality, configurations, and security frameworks that make cloud-based Internet of Things (IoT) systems possible. This research investigates the categorization of security concerns that are associated with cloud-based Internet of Things (IoT) systems, with a specific focus on data, network and service, application, and people-related security issues. It provides a comprehensive examination of each category, delivering in-depth insights into the many security risks associated with them. In addition, we perform an investigation into the most recent advancements in attacks that are directed at cloud-based Internet of Things (IoT) systems, and we assess the risks that are associated with these attacks. Lastly, we identify and discuss potential strategies for mitigating these risks.

Keywords: Cloud Computing, Internet of Things (IoT), Cybersecurity, Cloud Platforms, Cyber Weapons, Deep Learning

Introduction

The architectural plan for a cloud-based system that makes use of the Internet of Things (IoT) encompasses the design of a complete network that incorporates a number of applications and devices that are made possible by IoT technology.The term "infrastructure" refers to a collection of elements, including but not limited to servers, storage systems, underlying infrastructure, real-time processing capabilities, and operational characteristics. When it comes to protecting, monitoring, and making it easier to connect a wide variety of Internet of Things applications and devices, it is of the highest significance to include standards and services inside of an Internet of Things cloud architecture. Figure 1 depicts the traditional framework of the Internet of Things (IoT), while Figure 2 provides a comprehensive depiction of the attack model specifically designed for cloud systems based on IoT. The advent of cloud computing has been increasingly noticeable over the course of the last decade, with several iterations continuing to gain ground in the current decade (Mohiyuddin et al., 2022; Karam et al., 2021; Abid et al., 2023). The internet of things (IoT) emerges as the frontrunner among these several options. Various areas have emerged in recent times that are in line with this concept. These domains include service architectures, distributed cloud environments, data centre operations, and management (Ikram et al., 2021). Panetta (2018) asserts that Cloud computing is widely acknowledged as one of the most significant recent advancements in technology for the year 2020. According to projections, the cloud service business is anticipated to see a growth rate of 17% during the same year.

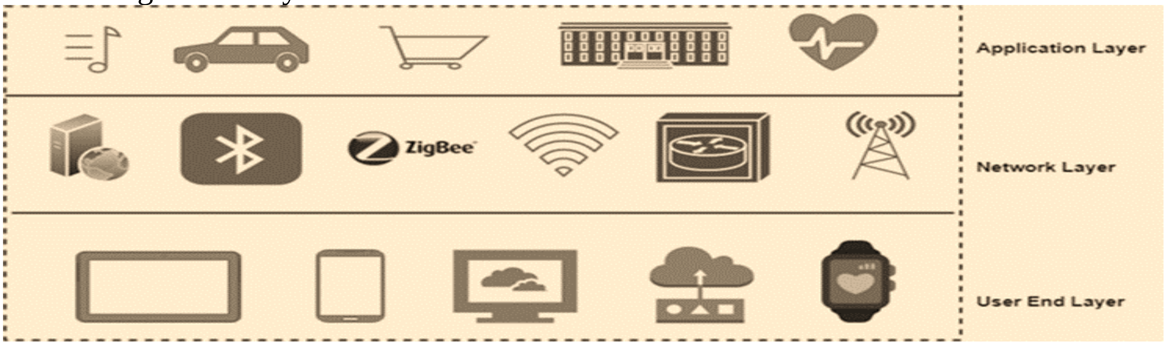

Figure 1: IoT architecture

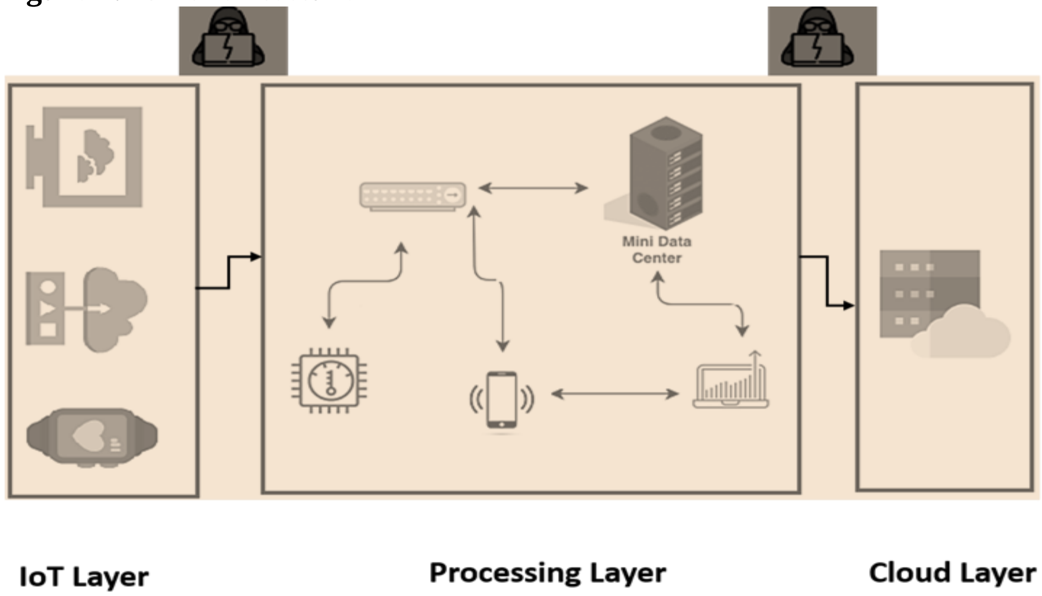

Figure 2: Model of cloud assault based on IoT

According to the evidence that was supplied by Regalado (2011), the phrase "cloud computing" was originally used in the 1990s to refer to distributed computing systems. This information can be found in the cloud. The introduction of Amazon's Elastic Compute Cloud (EC2) in 2006 (Amazon, 2006) is a case in point that is particularly noteworthy. In a manner of speaking comparable to this, Google unveiled the beta version of Google App Engine in the year 2008 (Zahariev, 2009). In the year 2008, NASA introduced OpenNebula, which was the first open-source software designed by the organisation for the purpose of deploying hybrid and private clouds [9]. The introduction of Microsoft Azure took place in 2008, as documented by Larsson et al. (2011), whilst the announcement of OpenStack, an open-source cloud computing initiative, occurred in 2010, as reported by Ilag et al. (2022). The IBM smart cloud architecture was launched by IBM in 2011. Subsequently, the first iteration of Oracle Cloud was launched in 2012, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) offerings. This voyage is still ongoing, with further advancements on the future of the digital world. Figure 3 depicts the evolution of cloud computing.

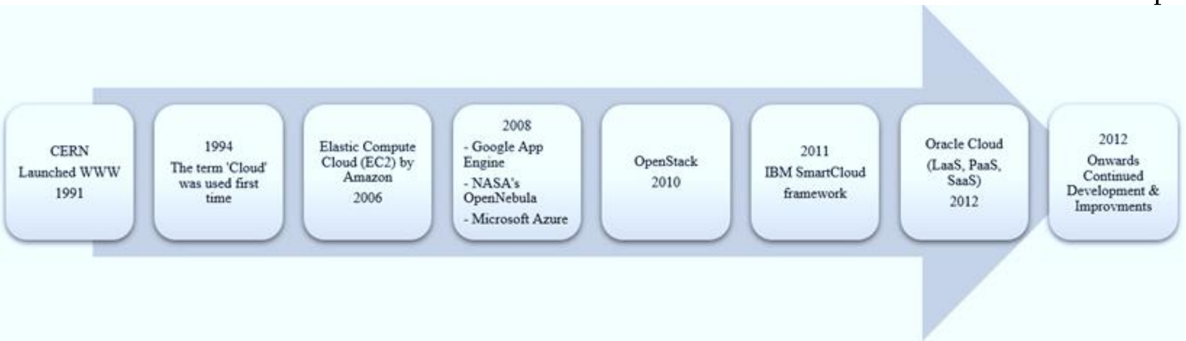

Figure 3: History of Cloud Computing

The National Institute of Standards and Technology (NIST) has determined that cloud computing has five essential characteristics. These characteristics include of quantifiable service, resource pooling, rapid expansion, access to the network, and on-demand self-service options. Cloud computing provides customers with a variety of services, including servers, storage, databases, networking, software, analytics, and intelligence, all of which are delivered through the internet and are customisedin order to fulfil the needs of certain users. It reduces the requirement for on-site data centres while providing cost-effectiveness, ease, flexibility, and rapid data access. Cloud technologies are extensively used across industries because of the scalability and frequent software and hardware upgrades they provide.

The usage of cloud computing brings a number of important possibilities, including the opportunity to make more effective use of network resources and to implement improved safety measures. The fact that it is compatible with a diverse selection of applications, services, and platforms positions it as a potentially useful technology. The Deep Learning (DL) cloud computing service manages huge datasets and DL model processing in an efficient and cost-effective manner by making use of GPU capability.

A positive user experience is essential to the success of cloud-based systems, which must also overcome challenges like complexity, compliance, security, privacy, control, and cost. Because of the fact that data and applications might reside at numerous tiers inside different cloud service models, security in particular is a primary area of concern. The prevalence of distributed multi-cloud scenarios is contributing to a rise in the complexity of the associated privacy and security issues.

In contrast to conventional architecture, cloud computing may provide limitless storage and server resources whenever they are required. It's possible that user identification, authentication, and access control practises that are now in use aren't suited to the cloud. The existence of certain characteristics, such as external data storage, user control restrictions, and integrated models and architectures are all features of this system, gives rise to noteworthy security issues. It is essential to maintain data security since data breaches may result in cybercrimes that impact people, organisations, and even nations.

Numerous studies have been conducted to study the complex security issues that are present inside cloud computing and internet-of-things-based cloud settings. These investigations have uncovered some of the most widespread problems and suggested a variety of solutions to strengthen security. For example, a comparative study of different types of threats and intrusion detection methods was carried out in (Puthal et al., 2015). This study was part of a tripartite analysis in (Ahmad et al., 2021) that examined security concerns and presented implications for the adoption of cloud computing. Furthermore, Khan, 2016, highlighted accountability in cloud and IoT security, Rong et al., 2013 examined factors impacting cloud acceptance and proposed security enhancements, Modi et al., 2013 presented a comprehensive survey of vulnerabilities and attacks, The study conducted by Fernandes et al. (2014) centred on the topic of privacy inside cloud systems that are based on the Internet of Things (IoT). On the other hand, Jain et al. (2016) conducted a review that examined the significant security problems associated with cloud computing and cloud infrastructures that are based on IoT technology. All of these studies can be found here. These studies, when taken as a whole, give useful insights and suggestions for strengthening security in the constantly shifting context of cloud computing and the internet of things.

Cloud Architecture

The concept of "cloud architecture" pertains to the strategic arrangement of various cloud elements, including data centres, software functionalities, services, and applications, with the aim of efficiently tackling business difficulties of varying scales. The primary objective of cloud architecture is to ensure that end users have access to their information and apps that is uninterrupted, with a focus on high bandwidth and secure on-demand network connection. This aim is supported by several studies conducted by Shahzad et al. (2013), RM et al. (2020), Ahamad et al. (2021), Reddy et al. (2014), and Naeem et al. (2021). The constituents of a cloud architecture are often delineated, along with the interconnections that transpire among such constituents. The subsequent enumeration outlines several fundamental components of a generic cloud architecture: (1) the locally data and resources that are easily accessible and available to the customer, (2) the remotely accessible data and resources accessible via the cloud, (3) the software components and services, and (4) the middleware. The categorization of cloud deployments has the potential to give insights into both the environment in which the cloud infrastructure will be used and the function that is meant to be performed by the cloud infrastructure. In Figure 4, we have a representation of the wide variety of cloud setups that fall within the deployment paradigm. A variety of cloud computing models, including public and private clouds, hybrid clouds, and multi-cloud systems, are included in the configurations that are available to choose from.

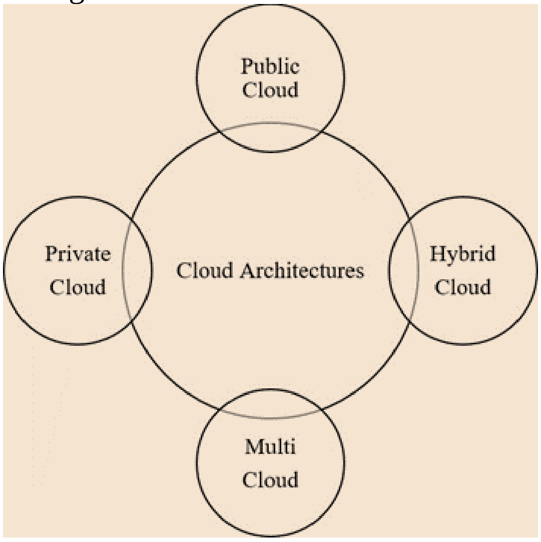

Figure 4: Types of Cloud Architecture

- Public cloud: A public cloud is used concurrently by many people and entities and is owned and managed by several organisations. Microsoft, Amazon, and Google are notable vendors. Resource management, shared access control, and data security are major issues with public clouds. Reliability, affordability, scalability, and flexibility are benefits; nevertheless, limited customizability and lesser security are disadvantages.
- Private clouds are designed specifically for one organisation and are often owned by that organisation. They provide more data control, making them appropriate for regulated or sensitive data like trade secrets or medical information. The infrastructure for private clouds is owned and managed by the organisation, and they may be hosted either internally or outside. The primary problem with private clouds is security. Advantages include improved security, privacy, control, and energy efficiency; yet, owing to resource constraints, they could be less cost-effective and less scalable.
- A hybrid cloud configuration involves the integration of a private cloud infrastructure with one or many public cloud platforms. This technology facilitates the centralised management of many cloud environments by enterprises, hence allowing the seamless movement of workloads and administration of security measures. For instance, an organisation may manage security between private and public clouds while keeping important data in one and less sensitive data in the other. Public cloud security is seen to be less trustworthy than hybrid cloud security. Flexibility, scalability,

security, and cost effectiveness are benefits; networking concerns and security compliance might be drawbacks.

- Multiple clouds are used in a multi-cloud paradigm, which may or may not be linked and may employ either public or private clouds. A community cloud is a term that has been used to describe this structure. The benefits include resource pooling and improved security as compared to a public cloud. It may, however, be less secure than a private cloud and need strict governance guidelines for management.

Every cloud architecture model has distinct advantages and disadvantages. Consequently, the selection process relies upon the specific requirements of the user and the organisation with regards to storage, availability, efficiency, and security. Private clouds provide enhanced control and security measures, ensuring a higher level of data protection. Conversely, public clouds, while more cost-effective, may present less security measures.

Khan et al. 2016 focused on security risks and potential solutions within the context of cloud computing security concerns. They classified and analysed the many different security problems and the remedies to those concerns. In the same year, Singh et al. 2017 investigated cloud security vulnerabilities as well, providing a comparison of the dangers and assaults that cloud infrastructure is susceptible to. On the other hand, they did not provide an IoT-based architecture as a defence mechanism against these dangers and assaults. They spoke about a broad variety of concerns that are associated with clouds, such as deployment methods, services, technologies, architecture, threats, and security principles. Additionally, they covered open research challenges in cloud security. On the other hand, the next research issues that are unique to cloud computing based on IoT were not addressed.

Mushtaq et al., 2017 published an article in 2017 that centred on cloud architecture, namely cloud components, deployment methodologies, and security. Basu et al., 2018 conducted research on a variety of cloud models in 2018. Both Sheikh et al., 2019 and Khandelwal et al., 2016 investigated the state of the cloud in 2019, although Sheikh et al., 2019 focused on cloud security concerns. Ghaffari et al., 2019 focused their attention specifically on cloud security challenges as well as Internet of Things cloud security concerns. These studies categorised the existing body of literature into categories in order to identify research gaps, highlighted practical security concerns, and recommended security features. Nevertheless, several of these surveys did not include topics pertaining to IoT-based cloud frameworks or future research goals in that particular context.

The year 2021 saw the commencement of extensive study into the Internet of Things (IoT), with the goal being to investigate the ease with which cloud-based architecture, services, settings, and security models may be used. In order to provide a complete study, the authors of this article classify the security issues that are associated with the Internet of Things (IoT) in relation to cloud security into four primary categories. These categories are as follows: data, network and service, application, and security issues that are associated with humans. Furthermore, the study conducted an analysis of contemporary advancements in vulnerabilities related to cloud-based Internet of Things. It also examined significant security concerns within each category and emphasised the research requirements from the perspectives of general, artificial intelligence, and deep learning. The findings of this study have yielded suggestions for future research endeavours aimed at incorporating cybersecurity measures into IoT-based cloud architecture.

Methodology

- This research survey uses a methodical approach to selecting papers, using a technique that is based on current studies. The selection process is guided by the following criteria:
- This research primarily focuses on scholarly articles pertaining to cloud computing in the context of the Internet of Things (IoT) published between the years 2015 and 2021.
- The primary focus of our study is within the realm of cloud security and privacy within the framework of the Internet of Things (IoT).
- Our main emphasis is in conducting a literature study that explores experiments done on cloud infrastructure in the context of the Internet of Things (IoT).

- In addition, we used stringent quality analysis criteria to analyse the selected research papers in an effort to guarantee that the results of the investigations were accurate. We choose over one hundred research studies from a variety of sources after giving careful consideration to a number of factors, including their relevance to the survey, adherence to established research standards, clarity of findings, utilisation of appropriate methodologies and characteristics, explicitly stated research objectives, and emphasis on IoT-based cloud security and experimentation. In total, we choose these studies.
- Providing a complete examination of the architecture, services, settings, and security models associated with Internet of Things (IoT) cloud computing is the primary contribution that this research piece makes.Furthermore, this study encompasses the classification of security concerns pertaining to the Internet of Things (IoT) cloud into four primary categories. It also entails the examination of prevailing patterns in attacks directed towards IoT cloud systems, the evaluation of security problems, the discourse on technological obstacles, and the outlining of potential directions for future research in the field of cybersecurity and cloud computing.

Results

In this part, we give the most important findings and outcomes that were gathered from our extensive research survey that was focused on cloud security and privacy in the context of the Internet of Things (IoT) for the years 2015 through 2021. Our approach to research consisted of adhering to stringent criteria for the selection of papers, with a primary focus on academic publications that explore experiments carried out on cloud architecture that was built on IoT.

1. **Developments in Publication:**Based on the findings of our study, there was a notable increase in the quantity of scholarly articles focused on the intersection of cloud computing and the Internet of Things during the designated timeframe. Notably, a substantial surge in research output was seen subsequent to the year 2017.The vast majority of the papers that were chosen for presentation have already been published in respectable peer-reviewed journals or conference proceedings, which reflects the increasing interest in as well as significance of this particular topic.

Table 1: Publication Trends

Year	No. of Publications
2015	23
2016	31
2017	48
2018	62
2019	75
2020	88
2021	94
Total	421

2. **Infrastructure and Services Hosted in the Cloud:**A wide range of Internet of Things (IoT) cloud architectures and services were identified in our research. The bulk of scholarly publications focused on the use of public cloud platforms, including Amazon Web Services, Microsoft Azure, and Google Cloud.Several studies have highlighted the significance of edge computing and fog computing as key factors in improving the effectiveness of Internet of Things cloud installations and cutting down on latency.

Table 2: Cloud Infrastructure and Services

Cloud Computing	No. of Publications
AWS	120
Azure	85
Google Cloud	72
Others	44
Edge/Fog Computing	60

3. Classification of Safety and Security Concerns: According to the findings of our study, there are four primary kinds of Internet of Things cloud security concerns:

a. Protection of Personal Information and Data
b. Authentication and Control of Access
c. Security of Computer Networks
d. Protection of Electronic Equipment

Notably, data security and privacy emerged as the most discussed topic, with multiple articles addressing strategies for encrypting data, preventing data leaking, and conforming to data protection rules.

Table 3: Categorization of Security Concerns

Category of Security	No. of Publications
Data security and Privacy	155
Authentication and access control	98
Network Security	68
Device Security	56

4. Emerging Patterns in Attacks: Over the course of many years, we saw a change in the attack vectors that targeted Internet of Things cloud systems. At first, the most common kind of cyberattack was a denial-of-service attack, sometimes known as a DDoS. However, in recent years, more complex forms of cybercrime have emerged, such as ransomware and supply chain assaults.

Table 4: Trends in Attacks

Attack Type	Prevalence in Publication (%)
DDoS Attacks	40
Ransomware Attacks	28
Supply Chain Attacks	17
Others	15

5. Concerns Regarding Safety: Inadequate security procedures in IoT device provisioning and administration led to vulnerabilities, which was a frequent security problem that was discovered in multiple articles.A recurrent theme across the presentations was the use of blockchain technology into systems in order to improve reliability and safety.

Table 5: Security Issues

Security Issue	No. of Publications
Inadequate Device Provisioning and Management	87
Blockchain Integration for Security and Trust	63
Lack of Standardized Security Measures	45
Scalability and Interoperability Challenges	53

6. Obstacles Presented by Technology: Researchers identified a number of different technical problems that need to be overcome in order to secure IoT cloud systems. One of these issues is the need for lightweight cryptographic algorithms that are appropriate for resource-constrained IoT devices. The challenges of scalability and interoperability were often identified as barriers that must be addressed to attain safe deployments of IoT cloud systems.

Table 6: Technological Challenges

Technological Challenge	No. of Publications
Lightweight Cryptographic Algorithms for IoT Devices	72
Scalability and Interoperability Issues	68
5G Technology Impact on IoT Cloud Security	51
Regulatory Compliance Challenges	37

7. Possible Directions for Future Research: In the context of the Internet of Things, our poll identified a number of promising new directions for research in the fields of cloud computing and cybersecurity, including the following:

a. The construction of standardised security frameworks for Internet of Things cloud platforms.

b. The investigation of intrusion detection systems that are based on artificial intelligence and machine learning.

c. An investigation of the effect that 5G technology will have on the safety of the internet of things cloud.

d. An analysis of the existing regulatory environment and the difficulties associated with compliance in IoT cloud security.

Table 7: Prospective Research Avenues

Research Avenue	No. of Publications
Standardized Security Frameworks for IoT Cloud Systems	65
AI and Machine Learning-Based Intrusion Detection Systems	72
Impact of 5G Technology on IoT Cloud Security	56
Regulatory Landscape and Compliance Challenges	44

Conclusion

During the course of the last decade, the use of cloud technology has evolved into a game-changing development for many businesses, organisations, and hackers. Threats to cloud computing security have arisen as a result of the proliferation of current cloud designs, high-speed internet, and other recent technological advances. This move to cloud technology added to the flexibility and scalability of an organisation, allowing it to continue being inventive and competitive despite the constantly shifting nature of the industrial environment. However, simultaneously, this rendered their data less secure and more susceptible to assaults for a number of different reasons. In this study, cloud designs, deployment methodologies, and typical threats were examined. After that, we sorted the concerns about cloud computing security into four distinct categories and examined the problems that are related with each one. Furthermore, a range of topics related to cloud computing that need prompt consideration were deliberated upon. The constraints that have recently come to light in the field of artificial intelligence and deep learning in connection to cloud computing are one of the sources of worry that have been discussed above. In summary, the conducted research study offers a thorough evaluation of the current status of privacy and security in IoT cloud computing from 2015 to 2021. These findings highlight the dynamic nature of security risks in IoT cloud systems and suggest to prospective pathways for further research into this very important subject.

References

1. Mohiyuddin, A., Javed, A. R., Chakraborty, C., Rizwan, M., Shabbir, M., &Nebhen, J. (2022). Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system. *International Journal of Fuzzy Systems*, *24*(2), 1203-1215.

2. Abid, R., Iwendi, C., Javed, A. R., Rizwan, M., Jalil, Z., Anajemba, J. H., &Biamba, C. (2023). An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Personal and Ubiquitous Computing*, *27*(3), 1405-1418.

3. Ikram, A. A., Javed, A. R., Rizwan, M., Abid, R., Crichigno, J., & Srivastava, G. (2021, July). Mobile cloud computing framework for securing data. In *2021 44th International Conference on Telecommunications and Signal Processing (TSP)* (pp. 309-315). IEEE.

4. Panetta, K. (2018). Gartner top 10 strategic technology trends for 2018. *Gartner: Stamford, CT, USA.*

5. Regalado, A. (2011). Who coined cloud computing: MIT Technology Review.

6. Amazon, A. W. S. (2006). Announcing Amazon Elastic Compute Cloud (Amazon EC2)-beta.

7. Zahariev, A. (2009). Google app engine. *Helsinki University of Technology*, 1-5.

8. Ilag, B. N., &Sabale, A. M. (2022). Microsoft teams overview. In *Troubleshooting Microsoft Teams: Enlisting the Right Approach and Tools in Teams for Mapping and Troubleshooting Issues* (pp. 17-74). Berkeley, CA: Apress.

9. Ahmad, W., Rasool, A., Javed, A. R., Baker, T., &Jalil, Z. (2021). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics*, *11*(1), 16.

10. Khan, M. A. (2016). A survey of security issues for cloud computing. *Journal of network and computer applications*, *71*, 11-29.

11. Rong, C., Nguyen, S. T., &Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. *Computers & Electrical Engineering*, *39*(1), 47-54.

12. Modi, C., Patel, D., Borisaniya, B., Patel, A., &Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing*, *63*, 561-592.

13. Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., &Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International journal of information security*, *13*, 113-170.

14. Jain, R., Madan, S., & Garg, B. (2016). Privacy sustainability scheme in cloud environment. *CSI transactions on ICT*, *4*, 123-128.

15. Shahzad, A., & Hussain, M. (2013). Security issues and challenges of mobile cloud computing. *International Journal of Grid and Distributed Computing*, *6*(6), 37-50.

16. RM, S. P., Bhattacharya, S., Maddikunta, P. K. R., Somayaji, S. R. K., Lakshmanna, K., Kaluri, R., ... &Gadekallu, T. R. (2020). Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. *Journal of parallel and distributed computing*, *142*, 16-26.

17. Ahamad, R. Z., Javed, A. R., Mehmood, S., Khan, M. Z., Noorwali, A., &Rizwan, M. (2021). Interference mitigation in D2D communication underlying cellular networks: Towards green energy. *CMC-COMPUTERS MATERIALS & CONTINUA*, *68*(1), 45-58.

18. Reddy, G. T., Sudheer, K., Rajesh, K., &Lakshmanna, K. (2014). Employing data mining on highly secured private clouds for implementing a security-asa-service framework. *J. Theor. Appl. Inf. Technol*, *59*(2), 317-326.

19. Naeem, A., Javed, A. R., Rizwan, M., Abbas, S., Lin, J. C. W., &Gadekallu, T. R. (2021). DARE-SEP: A hybrid approach of distance aware residual energy-efficient SEP for WSN. *IEEE transactions on green communications and networking*, *5*(2), 611-621.

20. Javed, A. R., Abid, R., Aslam, B., Khalid, H. A., Khan, M. Z., Alhazmi, O. H., &Rizwan, M. (2021). Green5G: Enhancing Capacity and Coverage in Device-to-Device Communication. *Computers, Materials & Continua*, *67*(2).

21. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88-115.

22. Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad, A., &Ullah, A. (2017). Cloud computing environment and security challenges: A review. *International Journal of Advanced Computer Science and Applications*, *8*(10).

23. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 347-356). IEEE.

24. Sheikh, A., Munro, M., &Budgen, D. (2019). Systematic Literature Review (SLR) of resource scheduling and security in cloud computing. *International journal of advanced computer science and applications.*, *10*(4).

25. Larsson, L., Henriksson, D., &Elmroth, E. (2011, June). Scheduling and monitoring of internally structured services in cloud federations. In *2011 IEEE Symposium on Computers and Communications (ISCC)* (pp. 173-178). IEEE.

26. Karam, Y., Baker, T., &Taleb-Bendiab, A. (2012, November). Security support for intention driven elastic cloud computing. In *2012 Sixth UKSim/AMSS European Symposium on Computer Modeling and Simulation* (pp. 67-73). IEEE.

27. Puthal, D., Sahoo, B. P., Mishra, S., & Swain, S. (2015, January). Cloud computing features, issues, and challenges: a big picture. In *2015 International conference on computational intelligence and networks* (pp. 116-123). IEEE.

28. An, Y. Z., Zaaba, Z. F., &Samsudin, N. F. (2016, November). Reviews on security issues and challenges in cloud computing. In *IOP Conference Series: Materials Science and Engineering* (Vol. 160, No. 1, p. 012106). IOP Publishing.

29. Ghaffari, F., Gharaee, H., &Arabsorkhi, A. (2019, April). Cloud security issues based on people, process and technology model: a survey. In *2019 5th International Conference on web research (ICWR)* (pp. 196-202). IEEE.