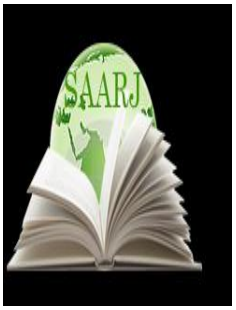
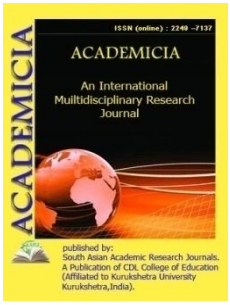


ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)



DOI: 10.5958/2249-7137.2021.02219.9

SECURE IOT AND CLOUD COMPUTING INTEGRATION

Ms Anuska Sharma*

*Sanskriti University,
Mathura, Uttar Pradesh, INDIA
Email id: anushka@sanskriti.edu.in

ABSTRACT

Mobile Cloud computing is a relatively new technology that refers to an infrastructure that stores and processes data outside of the mobile device. The Internet of Things is a relatively new technology. The Internet of Things (IoT) is a relatively new telecommunications technology that is quickly gaining traction. IoT is more particularly linked to wireless telecommunications. The primary aim of wireless network-based interaction and collaboration amongst things and objects is to achieve the goal established for them as a united entity. Furthermore, both Cloud Computing and the Internet of Things are rapidly developing technologies in the area of wireless communications. We provide a review of IoT and Cloud computing in this article, with an emphasis on the security concerns that both technologies face. We specifically integrate the two aforementioned technologies (Cloud Computing and IoT) in order to investigate the common characteristics and advantages of their integration. Finally, we will discuss Cloud Computing's contribution to IoT technologies. As a result, it demonstrates how Cloud Computing technology enhances IoT functionality. Finally, we look at the security issues that come with combining IoT with Cloud Computing.

KEYWORDS: *Internet of Things, Cloud Computing, Mobile Cloud Computing, Security, Privacy.*

1. INTRODUCTION

Mobile Cloud Computing is a relatively new technology that refers to an infrastructure that stores and processes data outside of the mobile device. The Internet of Things is a relatively new technology. The Internet of Things (IoT) is a relatively new telecommunications technology that is quickly gaining traction. IoT is more particularly linked to wireless telecommunications. The primary aim of wireless network-based interaction and collaboration amongst things and objects

is to achieve the goal established for them as a united entity. Furthermore, both Cloud Computing and the Internet of Things are rapidly developing technologies in the area of wireless communications. We provide a review of IoT and Cloud Computing in this article, with an emphasis on the security concerns that both technologies face. We specifically integrate the two aforementioned technologies (Cloud Computing and IoT) in order to investigate the common characteristics and advantages of their integration. Finally, we will discuss Cloud Computing's contribution to IoT technologies. As a result, it demonstrates how Cloud Computing technology enhances IoT functionality. Finally, we look at the security issues that come with combining IoT with Cloud Computing [1]. We study and analyze previous literature in the fields of cloud computing and Internet of Things, as well as their integration, for the purpose of this paper. The papers that made a significant contribution to our research are listed in the following paragraphs. To begin, provides an overview of the various security risks that pose a threat to the cloud. In addition, a survey was given in that was more specific to the various security issues that have arisen as a result of the nature of the service delivery models of a cloud computing system.

Moreover, an exploration \sof the roadblocks and solutions to provide a trustworthy cloud [2] computing environment presented in. Cloud computing is a rapidly evolving paradigm, but its unique characteristics exacerbating security and privacy concerns. Concerning the integration of Internet of Things and Cloud Computing, there have been made some \previous studies. proposes a new platform for providing and supporting ubiquitous connectivity and real-time applications and services for smart city needs using cloud computing capacities. In addition, shows a framework for data collected from highly distributed, heterogeneous, decentralized, real and virtual devices (sensors, actuators, smart devices) that can be managed, analyzed, and controlled automatically by distributed cloud-based services. The applications of IoT and CC in manufacturing are investigated in order to realize full sharing, free circulation, on-demand use, and optimal allocation of various manufacturing resources and capabilities. Furthermore, a CC- and IoT-based cloud manufacturing [3] (CMfg) service system (i.e. CCIoT-CMfg) and its architecture are proposed, and the relationship among CMfg, \sIoT, and CC is analyzed. Finally, discusses the benefits, challenges, and future work for the application and implementation of CCIoT-CMfg. The focuses on the Cloud of Things architecture, which is a common approach to integrating the Internet of Things (IoT) and Cloud Computing. Also, in review the state of the art for integrating Cloud Computing and the Internet of Things, and examine an IoT-enabled smart home scenario to analyze the IoT application requirements.

At the end, the Cloud Things architecture, a Cloud-based Internet of Things platform which accommodates Cloud Things IaaS, PaaS and SaaS for accelerating IoT application, development, and \management proposed in. In addition, includes a presentation and discussion of some of the IoT and Cloud Computing integration challenges that must be addressed in order to enable an intelligent transportation system to address issues such as high fuel prices, high CO_2 emissions, increasing traffic congestion, and improved road safety. is a demonstration of a method for developing Smart Home apps that integrates Internet of Things (IoT) with Web services and Cloud computing? [3]. The strategy focuses on four areas: embedding intelligence into sensors and actuators using the Arduino platform; networking smart things using ZigBee technology; facilitating interactions with smart things using Cloud services; and improving data exchange efficiency using the JSON data format. It also shows the implementation of three use cases, namely, assessing house conditions, monitoring home appliances, and regulating home access, to

illustrate the approach's practicality and efficiency. The offers a cloud-centric vision for global Internet of Things deployment. The most important enabling technologies and application areas that will likely drive IoT research in the near future are addressed. also shows a Cloud solution using Aneka that is built on the interplay between private and public Clouds.

Finally, it ends the IoT vision by emphasizing the need of bringing WSN, the Internet, and distributed computing together for the benefit of the technical research community. Because of the amount of data IoTs can generate and their requirement for virtual resource utilization and storage capacity, it's becoming increasingly important to integrate them with cloud computing, not only to make it possible to create more usefulness from the data generated by IoTs and develop smart applications for users, but also to make it possible to create more usefulness from the data generated by IoTs and develop smart applications for users. refers to this kind of connection as [2] Cloud of Things. Anything may become a part of the Internet and produce data with IoTs. Furthermore, in order to produce more useful services, the data created must be handled according to its requirements. Integration of IoTs with cloud computing is becoming more essential for the preceding aim. The Cloud of Things (CoTs) is the name given to this new paradigm. The authors' attention in is drawn to the combination of Cloud and IoT, which we refer to as the CloudIoT paradigm. In addition, numerous studies have looked at Cloud and IoT individually, as well as their major characteristics, features, underlying technology, and outstanding problems. These studies, on the other hand, lack a thorough examination of the new CloudIoT paradigm, which entails whole new applications, difficulties, and research concerns. focuses on some of the major problems in Cots and proposes smart gateway-based communication as a solution. Smart gateways are required for Cloud of Things to execute the sophisticated functions and preprocessing that sensors and light IoTs cannot. Finally, offers an overview of integration components, including cloud platforms, cloud infrastructures, and IoT middleware. There are also several integration ideas and data analytics methods discussed, as well as various difficulties and open research problems. Finally, we look at integration techniques and approaches for the technologies described above. The authors of concentrate [4] on Fuzzy C-Means based segmentation algorithms because of their high segmentation accuracy. Furthermore, the algorithms investigated need lengthy execution durations. In addition, the authors of use Graphics Process Unit (GPU) capabilities to speed up the execution time of these algorithms.

Finally, the authors obtain an increase in accomplishment performance of up to 8.9x without sacrificing segmentation accuracy. The primary goal of is to provide a review of the fundamental methodologies for such techniques and to identify new research trends in this field. The authors of describe several well-known techniques of face recognition in video sequences for biometric security applications and list new developments. In order to address the problem of a lack of research into effective and efficient evaluations and measurements for security and trustworthiness of various social media tools, platforms, and applications, surveys the state-of-the-art of social media network security and trustworthiness, particularly for the increasing sophistication and variety of attacks, as well as the reliability of various social media tools, platforms, and applications. In addition, the authors of emphasized a novel approach to assessing and monitoring basic and underlying platforms. Furthermore, based on signaling theory and crowd computing, the authors suggest a hierarchical design for crowd assessments, which is critical for the social media ecosystem. Each paper's results and ideas are included in Table 1.

More specifically, in Table 1, relevant information linked to the year in which the review was published, the precise authors, and as a conclusion for each article the issues and solutions that they deal with could be seen separately for each related review that was examined [3].

2. DISCUSSION

The Internet of Things (IoT) is a network of devices that communicate, exchange, and utilize data from the physical world to offer services to people, businesses, and society. The objects things have unique IDs and may operate alone or in conjunction with other items or people (identifiers). In addition, the Internet of Things has a variety of applications in health, transportation, the environment, and energy, as well as various kinds of devices: sensors, wearable devices (watches, glasses), and home automation (domestics). What exactly does it imply when devices and sensors are connected and interact with one another? What impact will the Internet of Things have on our everyday lives? GPS systems, alarm systems, and thermostats all transmit and receive continuous data in order to track and automate our everyday actions. And there's the less obvious: mosaic, mugs, clothing, and other commonplace items may all connect to a network and transmit and receive data via the Internet. Businesses explore opportunities where streaming data can generate new markets in order to drive good change or to improve current offerings. The following are some examples of sectors that are at the center of these changes

a) Transportation-related smart solutions: Transportation-related smart solutions decrease traffic on the highways, reduce fuel consumption, prioritize car maintenance programs, and save lives.

b) Smart power grids with more renewable: Smart power grids with more renewable enhance system dependability while lowering customer costs, resulting in cheaper energy.

c) Patient monitoring through remote access: Patient monitoring by remote access enhances the quality of services, increases the number of individuals serviced, and saves money.

d) Sensors in houses and airports: Sensors in homes and airports, as well as in your shoes and doors, enhance safety by transmitting signals when they are left unattended for a length of time or when they are utilized at the incorrect time.

Engine monitoring sensors that identify and anticipate maintenance problems, enhance inventory replenishment, and even set priorities in scheduling maintenance work, repairs, and regional operations are all examples of engine monitoring sensors. The field of IoT security is concerned with the protection of linked devices and networks in the Internet of Things. The Internet of Things refers to the growing number of items and entities – referred to as things in this context – that are equipped with unique IDs and the capacity to autonomously transmit data across a network. Computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle-to-vehicle communication, and wearable computing devices account for a large portion of the growth in IoT communication. The primary issue is that, since networking appliances and other items are still a relatively new concept, security has not always been taken into account in product design. Embedded operating systems and software are often supplied alongside outdated and unpatched IoT devices[5]. Furthermore, buyers often forget to change the default passwords on smart gadgets, or if they do, do not use adequately secure passwords. An IoT device that has

to be directly accessible over the Internet should be segregated into its own network and network access should be limited to enhance security. The network segment should then be watched for possible abnormal traffic, and if there is an issue, action should be taken.

Since the IoT idea was originally suggested in the late 1990s, security experts have warned about the potential danger of huge numbers of unprotected devices connected to the Internet. The first IoT botnet was found in December 2013 by a researcher at Proofpoint, an enterprise security company. According to Proofpoint, devices other than PCs made up more than 25% of the botnet, including smart TVs, baby monitors, and other home gadgets.

2.1.APPLICATION

Cloud computing is the use of the Internet to offer computers, storage, services, and applications. In general, significant hardware and software improvements are needed to make smart phones more energy efficient and computationally competent. This necessitates collaboration between developers and manufacturers. Mobile cloud computing is described as the integration of cloud computing technologies with mobile devices in order to maximize the processing power, memory, storage, energy, and context awareness of the mobile devices. Mobile Cloud Computing technology is the result of multidisciplinary methods that combine mobile computing with cloud computing. As a result, mobile cloud computing is another name for this transdisciplinary area. The phrase Mobile Cloud may be seen from two perspectives: infrastructure-based and ad-hoc mobile cloud. The hardware architecture in an infrastructure-based mobile cloud stays static while providing services to mobile users. Nonetheless, many apps make use of cloud resources, but solely for storage and application-specific features like Apple's Siri (voice-activated personal assistant) and iCloud storage service. Figure 1 Shows The Cloud Computing Effect.

Figure 1 Shows The Cloud Computing Effect.

The Cloud Computing technology, like other technologies, has certain characteristics that define its operation. Following that, these characteristics are examined and described. Storage over the

Internet (Storage over the Internet) is a technological framework that utilizes Transmission Control Protocol/Internet Protocol (TCP/IP) networks to connect servers and storage devices, as well as to make storage solution implementation easier. Storage over Internet Protocol (SoIP) technology is another name for Storage over Internet technology. SoIP offers high-performance and scalable IP storage solutions by combining the finest storage and networking industry techniques. The primary goal of the Internet Service is to assist clients all over the globe in turning their dreams become realities by using the Internet's efficiency, speed, and ubiquity.

2.2.ADVANTAGES

Cloud Applications, or Applications over Internet as a scientific definition, are programs that can be written to do the job of a current manual task, or virtually anything, and which perform their job on a server (cloud server) via an internet connection rather than the traditional model of a program that must be installed and run on a local computer. Google apps, online banking, and Face book are some examples of sophisticated programs that operate in the cloud and accomplish amazing feats of computation for the unsuspecting user who just needs an internet connection and a browser Efficiency in Energy efficiency is defined as a method of controlling and limiting the increase of energy use. It may be more energy efficient to provide more services for the same energy input or to give the same services for less energy input. When a Compact Florescent Light (CFL) bulb consumes 1/3 to 1/5% less energy to generate the same amount of light as an incandescent bulb, the Compact Florescent Light (CFL) is regarded to be more energy efficient. Computationally Capable Computational cloud services take use of computationally demanding and ubiquitous mobile applications made possible by Mobile Cloud Computing technologies. As a consequence, a system is deemed computationally competent when it fulfills the criteria for delivering the desired outcomes by doing the necessary computations. Mobile Cloud Computing has certain drawbacks and limits that need be addressed throughout time to create a better and more perfect application. Before using this technology, a lot of companies, particularly smaller ones, must be aware of the restrictions. The security problem is one of the main concerns with Mobile Cloud Computing. Before using this technology, it's important to understand that all of the company's sensitive data will be handed over to a third-party cloud service provider. This may put the company's future in jeopardy. As a result, one must be fully certain that they are selecting the most dependable service provider, one who will protect the information entirely. Internet connectivity is essential for Mobile Cloud Computing. As a consequence, before using these services, the user should be assured that the outcome is favorable. Mobile Cloud Computing has a huge potential user base since owning a mobile device that is linked to the internet has become the standard in today's wireless environment Performance is another significant issue with Mobile Cloud Computing. Some users believe that performance is inferior to that of native apps. As a result, it's a good idea to verify with only one service provider and learn about their track record Latency is a term that refers to the (Delay)Latency (also known as turnaround time) in mobile cloud computing refers to the time it takes to offload a calculation and get the results from a nearby infrastructure or cloud. Data privacy is essential, and it is one of the major barriers preventing customers from embracing mobile cloud computing. As a result, in order for customers to trust the mobile cloud, application models must enable app development that includes privacy protection and implicit authentication methods [6].

2.3.WORKING

Cloud computing security, often known as cloud security, is a growing sub-domain of computer, network, and information security. It refers to a collection of rules, tools, and controls used to safeguard data, applications, and the cloud computing infrastructure [7] Users and businesses may store and process data in third-party data centers with the help of cloud computing and storage solutions The Cloud is used in a number of service types (SaaS, PaaS, and IaaS) and deployment [8] patterns (Private, Public, Hybrid, and Community) by businesses. Cloud computing is linked with a variety of security issues. Security problems encountered by cloud providers (organizations that offer software, platform, or infrastructure-as-a-service through the cloud) and security issues faced by their clients fall into two categories (companies or organizations who host applications or store data on the cloud) However, the burden of proof is shared. The supplier must guarantee that its infrastructure is safe, as well as their customers' data and apps, while the user must take steps to secure their application and utilize strong passwords and authentication methods. Encryption algorithms serve a critical role in ensuring safe network communication [9]. It is an important and essential instrument for data protection. The encryption method scrambles the data using "a key," and only the user has the key to decode the data. Symmetric key encryption is an essential encryption method that has been discovered via study. Only one key is needed to encrypt and decode data in symmetric key encryption. The AES algorithm is the most often employed in this encryption method. NIST has suggested that AES (Advanced Encryption Standard) be used to replace the DES algorithm. The only known successful attack against it is a brute force assault, in which the attacker attempts all possible character combinations to break the encryption. Block ciphers based on the AES algorithm. It features a configurable key length of 128, 192, or 256 bits, with 256 being the default. It encrypts 128-bit data blocks in 10, 12, or 14 rounds, depending on the key size. AES encryption is quick and adaptable, and it may be used on a variety of platforms, including mobile devices. AES has also been thoroughly tested for a wide range of security applications This work depicts a portion of the AES algorithm. This method utilizes the original key, which is a 4x4 matrix containing the number of bytes in either instance [10].

3. CONCLUSION

The Cloud Computing technology opens up a lot of opportunities, but it also has certain drawbacks. Cloud computing is a kind of infrastructure in which data storage and processing take place outside of the mobile device. In this article, we provide an overview of Internet of Things technology, as well as an explanation of how it works and how to utilize it. We also go through the key characteristics of Cloud Computing and the trade-offs that come with it. Cloud computing is a kind of infrastructure in which data is stored and processed outside of the mobile device. In addition, the Internet of Things is a relatively new technology that is quickly gaining traction in the telecommunications industry, particularly in the contemporary area of wireless telecommunications.

The primary aim of wireless network interactions and collaboration between things and objects is to achieve the goal set for them as a united entity. Furthermore, both Cloud Computing and the Internet of Things are fast developing technologies dependent on wireless network technology. We provide a review of IoT and Cloud Computing in this article, with an emphasis on the security concerns that both technologies face. We specifically integrate the two aforementioned

technologies (Cloud Computing and IoT) in order to investigate the common characteristics and find the advantages of integrating them. Finally, the role of Cloud Computing to IoT technology was discussed, as well as how Cloud Computing technology enhances IoT functionality. Finally, the suggested algorithm model was used to assess the security issues of the integration of IoT and Cloud Computing, as well as a presentation of how the two encryption algorithms that were employed contribute to the integration of IoT and Cloud Computing. Future study on the combination of those two technologies may be conducted in this area. In order to have a better integration model, the security problem must be addressed or reduced to a minimum due to the fast growth of both systems. These security issues discussed in this article may be used as a case study for future research with the aim of reducing them.

REFERENCES

1. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, 2018.

2. R. S. Sinha, Y. Wei, and S. H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Express*. 2017.

3. A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and iot integration: A systematic survey," *Sensors (Switzerland)*. 2018.

4. M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, 2018.

5. A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT Middleware: A Survey on Issues and Enabling Technologies," *IEEE Internet Things J.*, 2017.

6. R. A. Khan and A. S. K. Pathan, "The state-of-the-art wireless body area sensor networks: A survey," *Int. J. Distrib. Sens. Networks*, 2018.

7. H. M. Jawad, R. Nordin, S. K. Gharghan, A. M. Jawad, and M. Ismail, "Energy-efficient wireless sensor networks for precision agriculture: A review," *Sensors (Switzerland)*. 2017.

8. K. S. Mulyarchik and A. S. Polochanskiy, "Quality of service in wireless sensor networks," *Zhurnal Beloruss. Gos. Univ. Mat. Inform.*, 2017.

9. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*. 2016.

10. O. Ur-Rehman and N. Zivic, "Wireless communications," in *Signals and Communication Technology*, 2018.