Journal of IoT in Social, Mobile, Analytics, and Cloud (ISSN: 2582-1369)
www.irojournals.com/iroismac/

A Perspective Review of Security Issues in IoT with Cloud Environment

Subarna Shakya

Professor, Department of Electronics and Computer Engineering, Central Campus, Institute of Engineering, Pulchowk, Tribhuvan University, Pulchowk, Lalitpur, Nepal

E-mail: drss@ioe.edu.np

Abstract

The Internet of Things (IoT) is a paradigm that is rapidly growing in all important fields of telecommunications. Cloud computing is a computing technique that provides a large amount of storage space for data enhancement. The integration of IoT and cloud computing expands storage space for a larger number of users while maintaining the data communication between the different end users. By combining the computing and communication paradigms, this integration produces an efficient result. The main disadvantage is security, which is the most important issue nowadays. This review paper examines the various security issues and potential solutions in the integration of IoT and cloud computing. This review work finalizes light weight cryptography such as block cypher and authenticate cypher approaches, which helps to improve data storage for efficient communication between multi users.

Keywords: Security issues, cryptography techniques, IoT, cloud computing, data processing

1. Introduction

Internet of things is the most prominent technique for communication. It transmits the data without the help of human, in human to human and human to machine interactions. The term “thing” denotes the person, object, devices, sensors, or any transponder that acts as a medium. Based on the IP address, the network is connected to the thing, it makes an effective communication.

Cloud computing is a technique which helps to store more data with a high number of users. Cloud computing is categorized into four different types such as private cloud, public cloud, hybrid cloud and multi cloud. The components of the cloud computing include the following, which helps to provide the efficient solution for large storage space.

DOI: https://doi.org/10.36548/jismac.2022.2.002
Received: 19.05.2022, received in revised form: 19.06.2022, accepted: 05.07.2022, published: 15.07.2022

- Server
- Database
- Data analytics
- Software
- Network
- Storage Space

Cloud computing is the most efficient technique and it provides a big shift in many business models. The computing cost is very lesser and it does not require any installation of software and hardware. This provides the high storage space with the help of servers. Database helps to maintain the data in the server, and data analytics helps to search the data in the server. Networking helps for a communication between the users. The integration of IoT and cloud computing provides the effective and efficient communication in many domains such as medical, agricultural, industry, education and smart city.

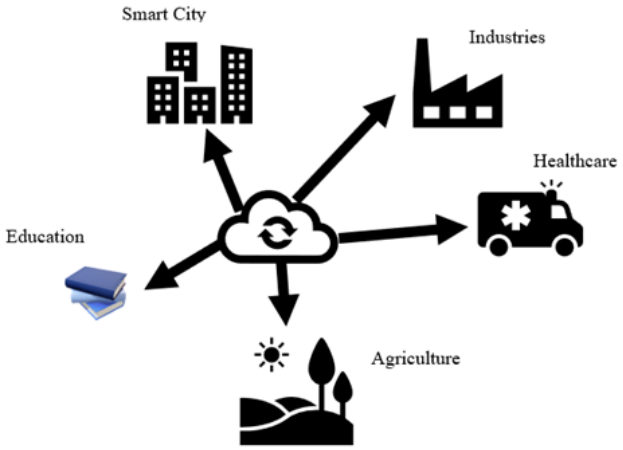

Figure 1. Integration of IoT and Cloud Computing

Figure 1 shows that the integration of IoT and cloud computing. IoT plays a vital role in all major fields by providing an efficient communication between the end-to-end users. The drawback included in the IoT communication is storage and space requirements. Integration of cloud computing with IoT provides an effective and efficient communication with multiusers.

2. Related Work

Stergiou et al., [1] presented the metrics included in the integration of IoT and cloud computing process. Additionally, it focused on the security issues, which has been overcome

by using the Advances Encryption Standard (AES) and Reed- Solomon Algorithm (RSA). The integration of cloud computing with the internet of things provides an effective solution and benefits to the IoT. Sadeeq et al., [2] provided the resolution of cloud integration issues with industrial internet of things. Cloud computing provided the bigger storage and internet of things provided the effective communication with large number of users. Biswas et al., [3] surveyed the research challenges and issues of cloud integration with internet of things. The review work exploded the centric cloud smart infrastructure integrated with the integrated internet of things and provided the solutions to overcome the integration issues. Aazam et al., [4] suggested cloud integration with IoT to overcome the sensor network issues and to cover large number of data users. This helped for an effective communication between the users.

Patil et al., [5] explained about the IoT application in agriculture domain and its vital role. IoT helps and simply the process of communication in the agriculture field. Due to the continuous monitoring and communication, it requires more storage space and that to be increased by using the integration of cloud computing technologies with IoT. This approach helps the farmer to make digital marketing via online and it reduces the cost and complexity. Surya et al., [6] discussed the security issues in the integration of IoT with cloud computing. While transmitting and storing the data, security is the most important concern. There is a possibility of multiple security issues to occur in the system. The survey work provided the possible solutions to overcome the security issues in the integration of IoT with cloud computing. Doukas et al., [7] explained the importance of integration of IoT with cloud computing in healthcare applications. In the medical field, high storage devices are required to store the sensed information while continuously monitoring the patient's health using sensors. The approach was applicable for wearable and mobile sensor devices and helped to increase the storage with efficient communication between the patient and doctor.

Wang et al., [8] introduced the scheme to avoid the bottle neck security issue in IoT with cloud computing based on the conventional modelling system. This system is fully automated, and it overcomes the bottle neck issue in the enterprise system. Mekala et al., [9] provided an efficient solution in the agricultural field with the integration of IoT with cloud computing. IoT helps to monitor the farming region and sense the required information like temperature, pH, water level and soil characterization. The review work helped to identify the best practice to implement the IoT, and cloud computing acted as a backbone to the wireless network. Mohiuddin et al., [10] explored the security challenges and issues in the IoT

integration with cloud computing. The review work suggested the possible solutions to overcome the third-party security issues and intruders.

2.1 Secure Integration Issues

Wang et al., [11] discussed about the internal attacks on the internet of things with the integration of cloud applications. The proposed trust security mechanism provided the efficient solution for the security issues. Additionally, it enhanced the efficient communication in the IoT- cloud services. Xu et al., [12] proposed the fine-grained access control technique to overcome the data security issues in the IoT cloud services. The approach focused on the data confidentiality and cryptosystems. The fine-grained access control scheme introduced the secret encryption and decryption key based on the time encoding system. The proposed approach provided an effective solution for a secure efficient communication. Almolhis et al., [13] explained the process of CloudIoT and provided the survey about the security issues in the cloud computing. The review work introduced the new class of security issues in the cloudIoT. Park et al., [14] defined the datagram transport layer security protocol, and it provided the secure communication between the users in the cloud environment. The security protocol is most suitable for UDP- and TCP-based applications.

Xiong et al., [15] proposed the ciphertext based policy-based attribution for secure communication in cloud computing environment for IoT applications. The approach reduced the storage use of public keys in the cryptography approach. Additionally, it reduced the computational overhead and storage cost compared to the existing approaches. Chakraborty et al., [16] introduced the distance and fuzzy based technique to avoid the MCDM problem. The approach provided an optimal solution and increased the efficiency for IoT based communication. Gupta et al., [17] presented the analysis in sustainable healthcare informatic. The research work focused on the real time patient monitoring and storing the data in cloud computing architecture. The cloud computing has three different architectures such as public cloud, private cloud and cloud data center. Security is maintained based on the encryption and decryption process. The approach is well suited for real time monitoring, and it provides an efficient communication.

Conti et al., [18] introduced the IoT based cloud framework for effective communication with end users by using Software defined network. The research work provided the flexible solution for the security issues. Jia et al., [19] proposed the secure truncating orthogonal frequency division multiplexing for the reduction of intercarrier

interference by using fast Fourier transform. Fernandez et al., [20] introduced the security patterns to overcome the security issues in IoT with cloud computing. Table 1 shows that comparison of different security techniques.

Table 1. Comparison of Secure Communication Techniques

Reference details	Technique	Methodology	Outcome
Al Sibahee et al. [21]	Lightweight security system	End to End and Smart to Smart IoT System communication	High security in real time applications
Sequeiros et al. [22]	Attack and system modelling	IoT based Cloud computing	Quality of solutions are improved
Tedeschi et al. [23]	Secure IoT Devices	Machine tools	Secure cloud system
Solapurkar et al. [24]	Authorization Framework (OAuth 2.0)	Healthcare services	Reduce secure storage overhead. Prevent the malicious attacks.
Moharana et al. [25]	Balanced incomplete block design model	Secure key management protocol	Secure end to end communication

3. Discussion

The integration of IoT and cloud computing provide an effective and efficient communication to the multi users. This approach provides an optimal solution for the storage issues and increases the users to communicate. The major drawback is the security, where there is a possibility of third-party access and intruders in the IoT networks. Security is the major concern issue in the integration of IoT and cloud computing. The survey explores the possibility of security issues and provide the optimal solution to overcome the security issues in the integration of IoT with cloud computing. The types of security core are given in the

figure 2 and it includes confidentiality, integrity, availability, authentication, authorization and accountability.

Figure 2. Security Core

The security issues occur due to the following reasons:

- There is a possibility of unauthorized communication between the users.
- The data leakage is possible while transmitting from cloud to IoT or vice versa.
- The Malware infection is found during the data transmission between the end users.
- The third-party access takes place while transmitting from public cloud service providers.

The necessary actions are to be taken to overcome the security issues in the IoT with cloud computing. The possible solutions are as follows. The proper authorized communication should be followed between the users. To avoid the third-party access, the encryption and decryption algorithm has to be included. Light weight encryption method provides an efficient solution over the security issues. To avoid the malware activities, authentication is to be followed while entering the user into the system. The login with username and password will be more helpful to avoid the malicious attacks. To avoid the data leakage, the encryption model has to be implemented. The lightweight cryptography technique provides a feasible solution to overcome the security issues. The lightweight cryptography technique contains block ciphers, hash functions, stream ciphers and authenticated ciphers. The lightweight block cipher technique is most suitable to tackle IoT security issues. The lightweight authentic cipher is most suitable for cloud computing security issues. The block cipher helps to overcome the communication issues and the authentic cipher enhances the data security in cloud computing.

4. Conclusion

This review work summarizes the security issues in the integration of IoT with cloud computing. IoT is the trendiest network and it attracts all users and makes smart communication between the users. Cloud computing is the most required technology for the more number of user with high storage capability. Integration of IoT with cloud computing

provide a tremendous support for high storage resource with an effective communication between multi users. The critical issue is security and it requires more attention for an effective communication. This review work analyses the possible security issues and provides the possible solutions to overcome the security issues in the integration of IoT with cloud computing. In future, the new encryption technique is to be introduced with the integration of block cipher and one time authenticate cipher. This approach would help to provide the solution for security issues and enhance the performance of IoT integration with cloud computing.

References

[1] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78 (2018): 964-975.

[2] Sadeeq, Mohammed Mohammed, Nasiba M. Abdulkareem, Subhi RM Zeebaree, Dindar Mikaeel Ahmed, Ahmed Saifullah Sami, and Rizgar R. Zebari. "IoT and Cloud computing issues, challenges and opportunities: A review." Qubahan Academic Journal 1, no. 2 (2021): 1-7.

[3] Biswas, Abdur Rahim, and Raffaele Giaffreda. "IoT and cloud convergence: Opportunities and challenges." In 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 375-376. IEEE, 2014.

[4] Aazam, Mohammad, Eui-Nam Huh, Marc St-Hilaire, Chung-Horng Lung, and Ioannis Lambadaris. "Cloud of things: integration of IoT

[5] Patil, V. C., K. A. Al-Gaadi, D. P. Biradar, and M. Rangaswamy. "Internet of things (Iot) and cloud computing for agriculture: An overview." Proceedings of agro-informatics and precision agriculture (AIPA 2012), India (2012): 292-296.

[6] Surya, Lakshmisri. "Security challenges and strategies for the IoT in cloud computing." International Journal of Innovations in Engineering Research and Technology ISSN (2016): 2394-3696.

[7] Doukas, Charalampos, and Ilias Maglogiannis. "Bringing IoT and cloud computing towards pervasive healthcare." In 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 922-926. IEEE, 2012.

[8] Wang, Chengen, Zhuming Bi, and Li Da Xu. "IoT and cloud computing in automation of assembly modeling systems." IEEE Transactions on Industrial Informatics 10, no. 2 (2014): 1426-1434.

[9] Mekala, Mahammad Shareef, and P. Viswanathan. "A Survey: Smart agriculture IoT with cloud computing." In 2017 international conference on microelectronic devices, circuits and systems (ICMDCS), pp. 1-7. IEEE, 2017.

[10] Mohiuddin, Irfan, and Ahmad Almogren. "Security challenges and strategies for the IoT in cloud computing." In 2020 11th International Conference on Information and Communication Systems (ICICS), pp. 367-372. IEEE, 2020.

[11] Wang, Tian, Guangxue Zhang, Anfeng Liu, Md Zakirul Alam Bhuiyan, and Qun Jin. "A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing." IEEE Internet of Things Journal 6, no. 3 (2018): 4831-4843.

[12] Xu, Shengmin, Guomin Yang, Yi Mu, and Ximeng Liu. "A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance." Future Generation Computer Systems 97 (2019): 284-294.

[13] Almolhis, Nawaf, Abdullah Mujawib Alashjaee, Salahaldeen Duraibi, Fahad Alqahtani, and Ahmed Nour Moussa. "The security issues in IoT-cloud: a review." In 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), pp. 191-196. IEEE, 2020.

[14] Park, Jiye, Hyeokjin Kwon, and Namhi Kang. "IoT–Cloud collaboration to establish a secure connection for lightweight devices." Wireless Networks 23, no. 3 (2017): 681-692.

[15] Xiong, Shuming, Qiang Ni, Liangmin Wang, and Qian Wang. "SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage." IEEE Internet of Things Journal 7, no. 4 (2020): 2914-2927.

[16] Chakraborty, Alakananda, Muskan Jindal, Mohammad R. Khosravi, Prabhishek Singh, Achyut Shankar, and Manoj Diwakar. "A secure IoT-based cloud platform selection using entropy distance approach and fuzzy set theory." Wireless Communications and Mobile Computing 2021 (2021).

[17] Gupta, Praveen Kumar, Bodhaswar T. Maharaj, and Reza Malekian. "A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres." Multimedia Tools and Applications 76, no. 18 (2017): 18489-18512.

[18] Conti, Mauro, Pallavi Kaliyar, and Chhagan Lal. "CENSOR: Cloud- enabled secure IoT architecture over SDN paradigm." Concurrency and Computation: Practice and Experience 31, no. 8 (2019): e4978.

[19] Jia, Min, Zhisheng Yin, Dongbo Li, Qing Guo, and Xuemai Gu. "Toward improved offloading efficiency of data transmission in the IoT-cloud by leveraging secure truncating OFDM." IEEE Internet of Things Journal 6, no. 3 (2018): 4252-4261.

[20] Fernandez, Eduardo B., Hironori Washizaki, Nobukazu Yoshioka, and Takao Okubo. "The design of secure IoT applications using patterns: State of the art and directions for research." Internet of Things 15 (2021): 100408.

[21] Al Sibahee, Mustafa A., Songfeng Lu, Zaid Ameen Abduljabbar, Xin Liu, Hemn Barzan Abdalla, Mohammed Abdulridha Hussain, Zaid Alaa Hussien, and Mudhafar Jalil Jassim Ghrabat. "Lightweight secure message delivery for e2e s2s communication in the iot-cloud system." IEEE Access 8 (2020): 218331-218347.

[22] Sequeiros, João BF, Francisco T. Chimuco, Musa G. Samaila, Mário M. Freire, and Pedro RM Inácio. "Attack and system modeling applied to IoT, cloud, and mobile ecosystems: embedding security by design." ACM Computing Surveys (CSUR) 53, no. 2 (2020): 1-32.

[23] Tedeschi, Stefano, Jörn Mehnen, Nikolaos Tapoglou, and Rajkumar Roy. "Secure IoT devices for the maintenance of machine tools." Procedia Cirp 59 (2017): 150-155.

[24] Solapurkar, Prajakta. "Building secure healthcare services using OAuth 2.0 and JSON web token in IOT cloud scenario." In 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), pp. 99-104. IEEE, 2016.

[25] Moharana, Soumya Ranjan, Vijay Kumar Jha, Anurag Satpathy, Sourav Kanti Addya, Ashok Kumar Turuk, and Banshidhar Majhi. "Secure key-distribution in IoT cloud networks." In 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS), pp. 197-202. IEEE, 2017.

Author's biography

Subarna Shakya holds Ph.D. in Computer Engineering from Lviv Polytechnic National University, Ukraine. He served as Executive Director at National Information technology Center, Government of Nepal and also head of Department of Electronics and Computer Engineering, Director of Center for Information Technology and Chairman of Electronics and Computer Engineering Subject Committee, Institute of Engineering, Tribhuvan University. He is Professor of Computer Engineering at Department of Electronics and Computer Engineering, Pulchowk Campus, Institute of Engineering, Tribhuvan University and also served as Visiting Professor in Brown University, Rhode Island, USA. He has published more than 120 technical and policy related papers in national as well as international reputed

journals. He was awarded by Nepal Education Leadership awards 2017, 18 Dec 2017 and outstanding contribution to education, 17 Dec 2018 by World CSR Day and World Sustainability. He was awarded 100 most dedicated professors, 4th July, 2019 and also awarded best professor in Computer Engineering studies, 10th Dec 2019 by World education congress. He was Conference Chair of Springer International Conference on mobile computing and sustainable informatics on 23-24 January 2020. He has organized many International conferences in Nepal such as Springer, IEEE related to security and Computing. He has already given key note speech related to Cloud computing and security in IEEE and Springer conference. He has given key note speech on different international conferences.