I.J. Wireless and Microwave Technologies, **2021, 4, 41-45**
Published Online August 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.04.05

Resource Efficient Security Mechanism for Cloud of Things

Adil Bashir and Sahil Sholla
Department of Computer Science & Engineering, Islamic University of Science and Technology, Kashmir, India
Email： adilbashir.445@gmail.com

Received: 30 May 2021; Revised: 09 June 2021; Accepted: 27 June 2021; Published: 08 August 2021

Abstract: Cloud of Things (CoT) relates to the convergence between Cloud Computing (CC) and the Internet of Things (IoT) and has significantly transformed the way services are delivered in the ubiquitous realm of devices. This integration has become essential because of the huge data being generated by IoT devices, requiring an infrastructure for storage and processing. Such infrastructure is provided by Cloud Computing services with massive space for data storage and exceptional platform to process complex data. IoT networks are vulnerable to multiple security breaches because of the growing usage of IoT devices in user personal systems. This leads to security and privacy threats that need to be addressed. IoT consists of resource limited devices which have feeble computing power, battery source and storage capacity. This paper addresses security issue by proposing usage of obfuscation and encryption techniques to scramble the data at IoT devices which is later on stored in encrypted form at the cloud server. The data at IoT devices is classified into highly critical or less critical and accordingly the appropriate technique between encryption and obfuscation is applied. The proposed mechanism is evaluated in terms of processing time for cryptographic operations at IoT devices. Evaluation results depict that the proposed mechanism is 1.17 times faster than [22] in terms of encryption and decryption times.

Index Terms: Cloud Computing, Cloud of Things, Encryption, Obfuscation, Internet of Things.

1. Introduction

Cloud Computing and Internet of Things have recognized an individualistic transformation. Although some mutual favors have been listed in the literature as a consequence of their merger and are anticipated in future. In particular, the Cloud provides a versatile tool for managing and designing IoT services, and even some applications that manipulate the stuff or the information that they generate [1]. From the other side, the Cloud takes advantage of IoT by extending its purview to cope with issues in the actual environment in the most suitable and efficient manner, and to introduce new services in various real-life scenarios. IoT finds applications in many fields such as smart Buildings, smart cities, smart agriculture etc [2]. Typically IoT is described by tiny devices in the modern world, widely distributed with finite storage and processing capabilities focusing on issues such as efficiency, output, and privacy protection [3, 4]. And from the other hand, cloud computing, having huge potential in terms of storing and processing power, is a highly developed technology which helps the IoT to partially solve its problems. Consequently, the current as well as future internet should be transformed by a new IT paradigm that combines these two complementary technologies.

Security is among the big concern that needs to be kept in mind while exchanging information in the Cloud-IoT environment [5]. The various security attacks by insiders and outsiders to IoT is because of its wireless nature. The on-going contact among the IoT devices or the IoT network and Cloud interface can be disrupted by an intruder [6-9]. Infected Cloud-IoT connectivity adversely affects secure and effective Cloud data storage. Meanwhile, Cloud usage to enable IoT data storage poses privacy issues by requiring all users to access information globally. There is a requirement of secure communication between IoT gadgets and Cloud framework, what is significant to protect person privacy and security within the CoT setting. The existing security mechanisms for CoT environment are complex and consume significant resources which is not feasible for IoT devices. IoT environment is characterized by constrained resources which are to be used efficiently in order to keep the devices functional for longer period of time. The work done in this paper address the security issue in Cloud-IoT environments by proposing an Authenticated-Encryption mechanism in order to safeguard sensitive data from attackers and requiring less time for cryptographic operations.

2. Literature Review

Zhu et al., [10] proposed a security scheme for the integration of Wireless Sensor Networks and Cloud computing and have elucidated its effectiveness in terms of design, functionality and security analysis. Authors in [11] proposed a secure architecture for Cloud-IoT that allows users to access different applications in cloud irrespective of the location and time. Further, the proposed scheme employs Elliptic Curve Cryptography (ECC) to mitigate security attacks. In [12], the proposed architecture to achieve the availability is ascertained through the execution system based on the Open-STACK. To ensure availability, a template-based cloud framework has been proposed which can configure fault identification and recovery measures automatically according to different services and features. According to the characteristics and services, proposed method applications were allowed by the templates and the feasibility methods were demonstrated with the existing architecture via comparison. Authors in [13] proposed a mechanism to secure Cloud of Things in which they have focused on the security aspects of both the technologies i.e. Cloud Computing and Internet of Things. The paper presents list of benefits that are aimed by the integration of IoT and CC platforms. The authors have proposed a mechanism that enhances the security in CoT environment. Authors in [14] proposed a metadata based security mechanism for the data that is stored at the server. The encryption key is generated using metadata and the key generation time depends on the number of attributes in the metadata. The key generated in this method is secure but the time taken by key generation algorithm is large which keeps the sensitive data exposed for larger time. Authors in [15] have analyzed the impact of routing attacks on power consumption of devices in IoT based healthcare system and concluded that Convolution Neural Network (CNN) is able to detect such attacks which have negative impact on power consumption of IoT devices.

In [16], the authentication scheme has been in which the biometric parameters are combined with the user credentials. The additional key is generated for ECC algorithm for improving its security level. Normally in ECC, only two keys are created that are public and private however in improved ECC, an additional secret key is generated. This additional secret key achieves the requirements of security like low encryption, computation, and decryption time overhead. Researchers in [17] have proposed Counter Mode with Cipher Block Chaining Message Authentication Code Protocol for providing security services in Cloud-IoT environment. Authors in [18], proposed the concept of secure trusted things that aims to reduce the security and privacy concerns in Cloud-IoT systems. It includes the encryption mechanism that involves less overhead. Authors in [19] have proposed a lightweight security scheme for IoT wherein the energy efficient and simple cryptographic operations are used. Authors in [20] proposed a security scheme for smart home systems based on Cloud-IoT infrastructure. It proposes group key management for smart home system. Here the proposed scheme ensures the secure data transfer via symmetric key cryptography. The analysis of proposed security scheme depicts that it is easy to implement, energy efficient and flexible. Authors in [21] have proposed an effective security scheme against DDoS attack in mobile-cloud computing environment. The authors in [22] have proposed secure data sharing for cloud assisted Internet of Things that uses secret key encryption with AES, public ley encryption with RSA and hash using SHA-256. The mechanism uses three different algorithms for securing critical data at IoT devices; however, the proposed mechanism incurs lot of overhead and is complex for resource constricted IoT devices.

3. Proposed Security Mechanism

In this paper, we provide an Authenticated-Encryption mechanism for Cloud of Things based on standard protocols and standards. Along with the encryption protocol, the proposed mechanism also employs the obfuscation technique in order to enhance the security in Cloud of Things. In developing the proposed solution, we have classified the IoT devices into highly critical data generators and less critical data generators. For example, in a smart home application system, every gadget is monitored and controlled over the internet. The gadgets may include the temperature sensor, humidity sensor, fire alarm sensor, medical sensors (attached to patient for his continuous observation). Among these devices or sensors, fire alarm sensor and medical sensors are classified as highly critical data generators and temperature, humidity sensors are classified as less critical data generators. Therefore, if the data is highly critical we use strong encryption mechanism and if the data is less critical, we use simple technique to obscure the data in order to preserve limited resources available at IoT devices. To achieve Authenticated-Encryption, the proposed mechanism uses AES-GCM [23] as cryptographic construct. Obfuscation technique is used through programming constructs and mathematical functions. Several obfuscation techniques are available which can be used to obscure the data. The research work in this paper uses two mathematical functions i.e. floor function and root function to obscure the input data.

The proposed algorithm determines the type of data (D) that is available at IoT devices. Depending upon the type of data, the appropriate technique between obfuscation and encryption is used to scramble the data. If the data (D) is less critical data, then obfuscation technique is used and if the data is highly critical data, then encryption is used. The proposed algorithm used in this research work is presented below.

```
Step 1: Sensed data (D) at IoT device (Input data).
Step 2: If D if critical data, go to step 3, else go to step 4
Step 3: Run AES-GCM algorithm to encrypt data and go to step 5.
    i.e. if D = critical_data() then
            AES-GCM_encryption(D)
Step 4: Run Obfuscation algorithm to obscure the data and go to step 5.
    i.e. if D = less_critical_data() then
            obfuscation(D)
Step 5: Transmit the data to Cloud Storage.
```

The algorithm is run at each of IoT devices before data is forwarded to cloud storage in order to scramble the data with appropriate technique.

4. Results

The proposed security mechanism provides Authenticated-Encryption service which provides confidentiality, authentication and integrity services to the highly critical data. The implementation has been done using PyCrypto toolkit [24]. We analyzed the performance of implemented mechanisms on Windows 7 64-bit intel i5 processor 2.60 GHz with 4-GB RAM and 320-GB storage. The proposed security mechanism has been evaluated and compared in terms of processing time with the mechanism in [22]. The comparison of encryption times and decryption times for different data sizes is shown in figure 1 and figure 2 respectively.

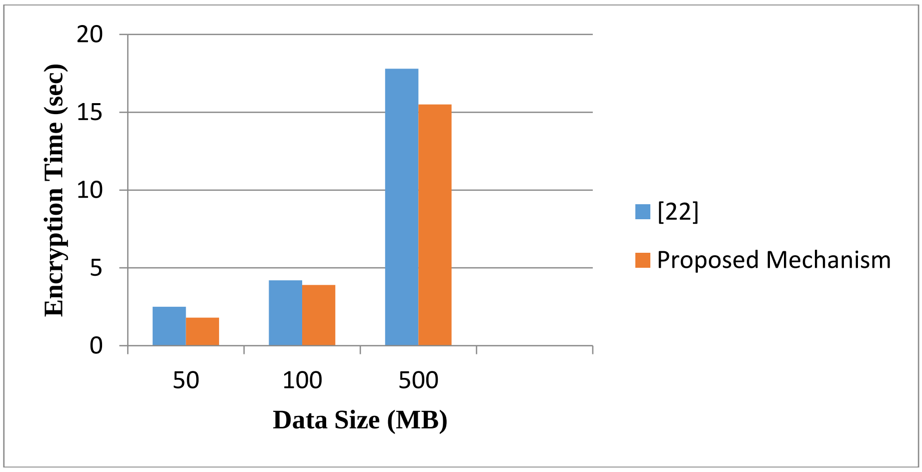

Fig. 1. Encryption Times Comparison

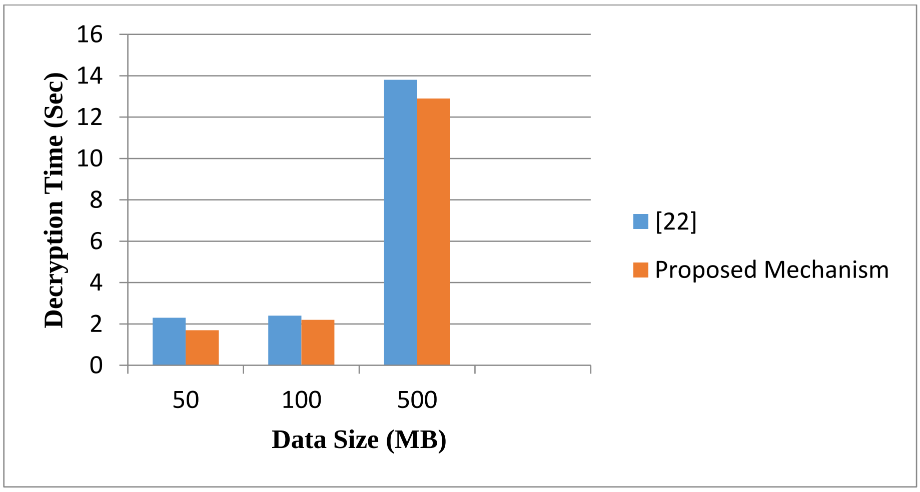

Fig. 2. Decryption Times Comparison

The implementation results show that the proposed mechanism reduces the processing time required for performing cryptographic operations as compared to [22]. Reduction in cryptographic processing time implies that the sensitive information available at IoT devices are encrypted quickly which reduces the time window available for attackers to get the unencrypted information. Furthermore, it also improves the lifetime of IoT devices by consuming less energy for the process.

5. Conclusion

Cloud of Things is an evolving area where two giant technologies are being integrated to provide mutual benefits to each other. Cloud computing provides different service benefits to IoT on one side and on the other side; IoT lets cloud computing reach to real world objects. The integration of Cloud and IoT put forth lot of research issues and the important issue among them is of security. In this paper, we tried to address the issue of security by proposing an Authenticated-Encryption mechanism for Cloud of Things so as to enable smart IoT devices to share data securely with other devices and requiring less time for cryptographic processing. The comparative analysis demonstrates that the proposed mechanism is 1.17 times efficient in terms of processing time compared to [22]. In future work, we plan on improving access control for the devices and the IoT data at the cloud.

Acknowledgement

This research work is funded under the seed grant initiative of TEQIP-III project currently being implemented at Islamic university of Science and Technology, Awantipora, Jammu and Kashmir.

References

[1] M. D íaz, C. Mart ín, B. Rubio, State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing, J. Netw. Comput. Appl. 67 (2016) 99–117.

[2] R. Mondal, T. Zulfi, “Internet of Things and Wireless Sensor Network for Smart Cities”, IJCSI International Journal of Computer Science Issues, Volume 14, Issue 5, September 2017.

[3] F. Khedim, N. Labraoui, A.A.A. Ari, A cognitive chronometry strategy associated with a revised cloud model to deal with the dishonest recommendations attacks in wireless sensor networks, J. Netw.Comput. Appl. 123 (2018) 42–56.

[4] N. Labraoui, M. Gueroui, L. Sekhri, A risk-aware reputation-based trust management in wireless sensor networks, Wireless Pers. Commun. 87 (3) (2016) 1037–1055.

[5] A. Khanna, An architectural design for cloud of things, FactaUniversitatis Series: Electron. Energ. 29 (3) (2015) 357–365.

[6] M.S. Ferdous, R. Hussein, A. MadiniAlassafi, R. Walters, G. Wills, Threat taxonomy for Cloud of Things, Internet of Things and Big Data Analysis: Recent Trends and Challenges 1 (2016) 149–191.

[7] T. Bhattasali, R. Chaki, N. Chaki, Secure and trusted cloud of things, in: 2013 Annual IEEE India Conference (INDICON), IEEE, 2013, pp. 1–6.

[8] M. Babaghayou, N. Labraoui, A.A.A. Ari, EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks, in: 3rd edition of the National Study Day on Research on Computer Sciences (JERI2019), Saida, Algeria, 2019.http://ceur-ws.org/Vol-2351/paper_67.pdf.

[9] S. Pearson, Privacy, security and trust in cloud computing, in: Privacy and Security for Cloud Computing, Springer, 2013, pp. 3–42.

[10] C. Zhu, H. Nicanfar, V.C. Leung, L.T. Yang, An authenticated trust and reputation calculation and management system for cloud and Sensor Networks Integration, IEEE Trans. Inf. Forensics Secur. 10 (1) (2015) 118–131.

[11] T.D.P. Bai, S.A. Rabara, Design and development of integrated, secured and intelligent architecture for Internet of Things and Cloud Computing, in: 2015 3rd International Conference on Future Internet of Things and Cloud, IEEE, 2015, pp. 817–822.

[12] Y.Hyunsik& K. Young, “Design and Implementation of High-Availability Architecture for IoT-Cloud Services”, Sensors, vol. 19. No. 15, 2019.

[13] C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and cloud computing, Future Gen. Comput. Syst. 78 (2018) 964–975.

[14] R. Anitha, P. Pradeepan, P. Yogesh, and Saswati Mukherjee, “Data Storage Security in Cloud using Metadata”, 2nd International Conference on Machine Learning and Computer Science(IMLCS'2013), Kuala Lumpur (Malaysia), August 2013, pp 26-30.

[15] S. O. Kamel and S. A. Elhamayed, “Mitigating the Impact of IoT Routing Attacks on Power Consumption in IoT Healthcare Environment using Convolutional Neural Network”, I. J. Computer Network and Information Security, 2020, 4, 11-29.

[16] M. A. Khan, S. Member, and M. Y. Khan, “A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data,” IEEE Access, vol. 8, pp. 52018–52027, 2020.

[17] K. N. Mishra, “A Proficient Mechanism for Cloud Security Supervision in Distributive Computing Environment”, I. J. Computer Network and Information Security, 2020, 6, 57-77.

[18] A. Hameed and A. Alomary, "Security Issues in IoT: A Survey," 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 2019, pp. 1-5, doi: 10.1109/3ICT.2019.8910320.

[19] B. Adil & M. Ajaz, “Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol”, EAI Endorsed Transactions on Internet of Things. 3. 154390, 2018. doi: 10.4108/eai.6-4-2018.154390.

[20] B. Alohali, M. Merabti, K. Kifayat, A Secure Scheme for a Smart House Based on Cloud of Things (CoT), in: 2014 6th Computer Science and Electronic Engineering Conference (CEEC), IEEE, 2014, pp. 115–120.

[21] K. Sekarana , G. R. Vikramb , B.V. Chowdaryc, "Design of Effective Security Architecture for Mobile Cloud Computing to Prevent DDoS Attacks", I.J. Wireless and Microwave Technologies, 2019, 1, 43-51.

[22] M. B. Mollah, M. A. K. Azad and A. Vasilakos, "Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things," in IEEE Cloud Computing, vol. 4, no. 1, pp. 34-42, Jan.-Feb. 2017, doi: 10.1109/MCC.2017.9.

[23] AES-GCM authenticated encryption, AES with Galois/Counter Mode (AES-GCM), https://www.cryptosys.net/pki/manpki/pki_aesgcmauthencryption.html , accessed on 17-09-2020.

[24] PyCrypto - The Python Cryptography Toolkit, https://www.dlitz.net/software/pycrypto/, accessed on 18-09-2020.

Authors' Profiles

Adil Bashir received his Bachelor of Technology (B. Tech) in Computer science and Engineering from Islamic University of Science and Technology, Jammu and Kashmir, India in year 2011. He has done his Master of Technology (M. Tech) in Communication and Information Technology from National Institute of Technology (NIT) Srinagar, India in 2013. Presently, he is Assistant Professor in the Department of Computer Science and Engineering at Islamic University of Science and Technology, Awantipora, Kashmir. His research interests are Internet of Things, Wireless Sensor Networks, Embedded Systems and Network Security.

Sahil Sholla, is Assistant Professor at department of Computer Science & Engineering, Islamic University of Science and Technology Awantipora, Pulwama , J&K, India .He has received PhD from National Institute ofTechnology Srinagar, India. His research focuses on technology ethics, security and Internet of Things.

How to cite this paper: Adil Bashir, Sahil Sholla, " Resource Efficient Security Mechanism for Cloud of Things", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.4, pp. 41-45, 2021.DOI: 10.5815/ijwmt.2021.04.05