A Survey on IOT and Cloud Data Security

K.Sabarish[1], A.Sidharth[2], R.Sanjaykumar[3], K.Siddharthraju[4]

[1]*UG Scholar, Assistant Professor (Sr.G), Department of Electronics and Communication Engineering. 1 ksabarish10@gmail.com*
[2]*UG Scholar, Assistant Professor (Sr.G), Department of Electronics and Communication Engineering, 2sidharthnair200@gmail.com*
[3]*UG Scholar, Assistant Professor (Sr.G), Department of Electronics and Communication Engineering. 3sanjukrs98@gmail.com.*
[4]*Department of Electronics and Communication Engineering,KPR Institute of Engineering and Technology, Coimbatore.4k.siddharthraju@kpriet.ac.in*

Abstract

The internet of things (IoT) and cloud computing has an incredible impact and growth that is predicting to have billions of connected devices in the near futur0. However the IoT devices have limited storage and network capacity and are easily to hack in order to compromise this various data securities in cloud computing is used. In this paper, we present and survey many major security issues for the IoT using cloud computing. We categorise and also discussed about the different security issues with regards to the IoT and cloud computing using different layered architecture, network communication and also management. We outline existing security issues, architecture and also providing state-of-art solutions for IoT along with the cloud computing.

Key points : *IoT Data Security, Cloud Data Security, AES Algorithm , Cryptography, Encryption Decryption.*

I. Introdution

In the recent years , due to the rapid development of cloud users the cloud computing along with IoT as significantly growing. A key features of the IoT environment is the resource sharing provided by the cloud computing. A geographically independent cloud platform is used to support, access the data from the IoT and from the IoT devices and also able to access resources and data from any location. An essential and importance of the cloud computing technology is the cloud data security which is used to provide protection to the user's data. Some of the necessary features of the cloud computing and the IoT are the user's Authentication and secured data storage. Cloud storage is the important part of the cloud based techniques and the IoT technology provides basic features like resource cooling and accessing of algorithm. Due to the increase number of threats, shared infrastructure and unauthorised access to the data have been increased the IoT requires the new accessing control according to changing in environment which are provided by the cloud computing security. According to the environmental changes in the IoT various architectural designs and algorithms arises and hence the cloud computing has two main concerns : without the owner's permission an un authorised person can access the data in the IoT, the owners data is breached by any cloud service provider. . From a security perspective, this plethora of IoT devices flooding the world is having tremendous consequences, so that it is not an exaggeration to talk about a security and privacy disaster. Cloud Computing and the Internet of Things (IoT) – two paradigms which share many common features. The integration of these numerous concepts may facilitate and improve these technologies. The integration of cloud computing in to the IoT which involves the benefits from thr integration process and implementation challenges, thus the IoT systems nowadays strongly rely on cloud

and various end devices to collect data and to connect the powerful cloud servers. Thus it cloud be well said that cloud computing and the IoT will be the future of the internet and next generation technology.

II. Literature review

Patel et al.(2016) [1] in their paper proposed an algorithm for securing the data in the cloud using Elliptic Curve Cryptography (ECC) and Blowfish. They provide authentication and confidentiality they have integrated these two algorithms. Then compare to the blowfish algorithm this scheme has very less execution time. Hence when compared to the blowfish algorithm this scheme has very less execution time.

Talari BhanuTeja et al. (2017) in their paper "Encryption And Decryption – Data Security For Cloud Computing"[2] implemented using AES algorithms which are used for encryption and decryption. Secure uploading and downloading of files has been proposed. The spine structure is provided as advantage to the cloud storage frameworks where security issues are required to be decreased as much as possible. The main drawback is that the Proposed system works only on text files and not on data like image, audio, video, etc .

Rizky Riyaldhi et al. (2017) in their paper titled "Improvement of Advanced Encryption Standard Algorithm with Shift Row and S box Modification Mapping in Mix Column"[3] the shift row in circular process has caused the reduction and the S box modified for the mix column transformation has led to the improvement of the algorithm. The encryption process achieved 86.143% and the decryption process achieved 13.085% improvement. However, the proposed implementation consumes larger memory space to store two modified S Box map and Array Shift Row map.

Han et al [4] (2017) is proposed an effective and secure access control scheme to resolve the backward security, key escrow and also resolving the inefficiency problems in the existing attribute encryption technic. The attribute encryption technic is not be applied straight away to the cloud data storage because it has three problems. In this proposed system, the key generation centre is partitioned in to distributed semi trusted parts to tackle the key escrow and conclusion problem. However secrecy revocation algorithm is used to addresses the back secrecy problem and efficiency problem and the data stored securely.

Singh et al [5] (2017) in their paper titled "Efficient algorithm for data security in cloud storage" this proposed system provides us a efficient algorithm for securing the data ie saved in the cloud storage. The files that are to be uploaded to the cloud are encrypted by this algorithm. The integrity and confidentiality of the data uploaded by the user is ensured doubly by not only encrypting it but also providing access to the data only on successful authentication. The AES algorithm will encrypt the file present on the device and also will enhance the security. The ELGamal algorithm will encrypt the AES key and stored in the intern server therefore the proposed system allows the user to read as well as upload the encrypted filr on to the system.

Osman et al (2017)[6]in their paper proposed an enhanced version to improve the confidentiality in cloud computing with a new security scheme using the (ECC) elliptically curve cryptography. The primary advantage of the system is the high computational complexity and efficient mix up of data. Hence in this system the security of the cloud and the user confidentiality protection is ensure by encryption of the data .

Elumalaivasan et al - Muthurajkumar et al..(2017)[7][8] developed an efficient encryption technique to protect the data in decentralized disruption tolerant networks. They introduced the new and the secured temporal log management technique for cloud computing environment. Many works have done by the researchers in this direction. This work proposes a new model for providing security for the Cloud and IoT-based applications.

Du meng et al.(2018) in their paper titled "Data security in cloud computing" [9]the cloud computing provides two basic service model that are computing and data storage. To meet the user demands cloud computing needs high performance cloud storage. The data send from the user will be in encrypted file by using AES algorithm in the cloud storage. Hence the data are encrypted as a container thus encryption keys are required to access the data. This proposed method can also be used to categorise and segregate the data of identical sensitivity in to directory that are encrypted individually.

Khan, M. A., & Salah, K. (2018). IoT security Kothmayr et al 2017 in their paper titled "End To End security authentications IoT devices"[**10**] the public cryptography technic is used for the authentication process is categorise in to three IoT levels depending upon the high level , intermediate level and low level layer. In the low level layer the security issues deal with insecure encryption process of the data. The intermediate level layer deals with the security issues of end to end data storage in the IoT cryptography. The high level layer deals with the security issues from IoT to cloud data transferring ie securely stored in the cloud. However the diversity of resources in IoT are required for defining a robust global mechanism of IoT layers. The proposed system also outlines and identifies future and open research issues and challenges that need to be addressed by the research community in order to provide reliable, efficient, and scalable IoT security solutions

Yao et al. (2018) [**11**] proposed a concealed security storage pattern technique with symmetric encryption method. The famous cryptographic method used in this technique is symmetric encryption where it is used to support the search functionality on the cloud over the encrypted data. However most of the symmetric encryption scheme has the drawback of storage leakage problem. In this paper, the author has protected the leakage of storage pattern by uniquely bridging the cryptographic techniques of chameleon hashing and in distinguishability obfuscation.

Wang et al (2018) [**12**] proposed the symmetric encryption scheme using the AES algorithm. In this system the AES algorithm is used to recover the secret key from the pair of plane/cipher text

Zheng et al (2018) [**13**]in this paper in order to avoid the dynamic degradation and using a digital chaotic system and to reduce the cryptosystem a new light weight encryption methodology was proposed hence the result of security analysis the scheme is opposed to differential, linear, forgery, and tampering, statically attacks and also it has a large key space. Simulated results shows that the S-Box is adaptable, cost efficient and secured.

Xiang et al (2018)[**14**] he proposed a new cryptographic domain for performing effective encryption process using the water marking algorithm in this proposed system in order to improve the privacy level the data in the form of plane text is converted in to cipher text before uploading the content to the cloud

Wang, W., Xu, P., & Yang, L. T. et al (2018). [**15**] In their paper titled "Secure Data Collection, Storage and Access in Cloud-Assisted IoT." In the proposed system the cloud access IoT system is used to access the confidential data CIBPRE. With thw assistance of the cloud the user can shared his / her collected IoT data to the other user using the data access phase. At the same time, the cloud cannot disobey the user's request to share the nonexpected data with other users or share the expected data with non-intended users. Otherwise, the cloud can possibly know the users' data. However in this system if a user wants to share another users data he must access the identify data which was stored as an initial cipher texting cloud.

Hammami et al. (2018) [**16**] introduced a novel secure migration schema in which the data in the cloud are securely migrated anyplace in cloud using DNA cryptography. It improves the confidentiality and the integrity of data comparing to other schemes.

Kazim et al. titled "Secure and optimize data storage for IoT through cloud frame work"(2018) [**17**] the proposed system states that the data storage in IoT is two branched namely big data and personal data. With consumers using the applications and the devices learning more about the user, momentous data will be generated. The IoT is used to provide data stream and secluded assets to the centralized management system. These resources is now used to information on the data location using the new and existing organizational process. The problems in this proposed system is to resolve using a cloud computing as it is associated with the access and storage of IoT data. Since the users are already familiar with functioning and storage of cloud, they are more probable to choose to separate their data as it were and use their own, cloud storage for personal data while time-honored big data can be handled by the enterprise and possibly in the cloud as well.

Shao et al. (2018)[**18**] in their paper proposed the encryption technic which consists of cipher text master security key for constant using a new secure method for the cloud data storage. The cryptographic cloud storage has a basic requirement of these properties such as cipher text master key security and cipher text security.by using these properties the data will be stored securely and the data will be encrypted and store to the cloud.

Zheng et al. [19] (2018)developed a new encryption methodology which is lightweight and authenticated to avoid dynamic degradation and to reduce the cryptosystem with disorder in a digital chaotic system. As a result of security analysis the scheme is opposed to differential, linear, forgery, and tampering, statically attacks and also it has a large key space. Simulated results shows that the S-Box is adaptable, cost efficient and secured.

Fu, J., Liu, Y., Chao, H.-C., Bhargava, B., (2018) [20] In their paper titled Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing in this system a public key and a secret key is assigned to IoT node with a unique identities. To enable the data transfer security between two nodes each pair of the neighbouring node generates the shared session key. The edge server consists of a session key with each IoT node. If the adversary scatters some malicious nodes into the network to act as the common IoT nodes, they cannot negotiate the session key with any IoT node considering that they don't have the legal identity, public key and secret key. Using the compromised nodes only the local data is obtained rather than all the data received by some IoT nodes.

T.Ramaporkalai et al.(2018) [21] in their paper proposed the data can be hacked by an un authorized person while transferring the data some of the major issues related to the data security include data integrity, data availability, data confidentiality, privacy, transparency of data and control over data where data resides. Various encryption method and access control are used to provide data security. Hence in this proposed system the infrastructure provided by the service provider mus be secured and clients data should remains protected.

Ni J Zhang K Lin X Shen X 2018 in their paper titled "Secured cloud storage system for storing IoT data"[22] the IoT data is stored in a cryptographic technic the data is sent in the form of a plane text the plane text is assigned as a symmetric key data. The IoT data which is uploaded on the cloud is more secure using the symmetric key cryptographic algorithm. The asp.net is used to design a secure cloud storage system. The encryption process takes place Using the cryptographic technique the symmetric text is now subjected to various encryption rounds where shift rows and mix columns takes place. Now the encrypted symmetric text is sent to the cloud storage now to access the encrypted symmetric key then he/she adds the user in the system to access the stored data according to their needs from the cloud storage. Hence the cryptographic symmetric key technic is used to store the data from the IoT to the cloud storage.

Zhang, Z. (2018).[23] In their paper data security in cloud using edge server and proxy server. In this system once the data packages are encrypted then the edge server decrypts then and process them according to the present instruction now the edge server is used to store the time limited data. Before the data and the indexed structure are being outsourced to the cloud server they are encrypted by the proxy server. Hence in this system in order for the cipher text to be protected from leaking they are encrypted by asymmetric encryption before delivering the cipher text to the cloud server.

Jiang et al (2019). In their paper titled "Secured Storage on Cloud and Security on IoT Devices"[24] the re-encryption technology for the secure cloud storage is broadcasted by proposing and encrypted data sharing method with conditional proxy. The dynamic sharing along with the broadcast data sharing is also used in this scheme. The dynamic sharing is nothing but the process in which the user in which added or removes from the sharing groups without any change in their encryption public scheme. Hence in the proposed system the encrypted text is shared with the target user using the re-encryption technology.

III. Conclusion

In this paper we have discussed about the various techniques to store the data securely in cloud computing and IoT devices. Today IoT devices are in secure and incapable of defending themselves mainly due to the unauthorised access of data and immature network standard. However the following research, we survey and review many IoT and cloud security issues depending upon different IoT and cloud layers. So the above mentioned security issues , threats and their solutions play a vital role and also form the basic necessity for IoT and Cloud.

References

[1] P. Patel , R. Patel , N. Patel , Integrated ECC and blowfish for smartphone security, Phys. Procedia 78 (December 2015) (2016) 210–216 .

[2] Talari Bhanu Teja, Vootla Hemalatha,K Priyanka, "Encryption And Decryption – Data Security For Cloud Computing – Using Aes Algorithm", SSRG International Jour

[3] nal of Computer Trends and Technology (IJCTT) ,Special Issue , pp 80-83, April 2017.

[4] Riyaldhi, R., Rojali, & Kurniawan, A. (2017). *Improvement of Advanced Encryption Standard Algorithm With Shift Row and S.Box Modification Mapping in Mix Column. Procedia Computer Science, 116, 401–407.* doi:10.1016/j.procs.2017.10.079

[5] K. Han , Q. Li , Z. Deng ,Security and efficiency data sharing scheme for cloud storage, Chaos Solitons Fractals 86 (2017) 107–116 .

[6] J. Singh , T. Pasquier , J. Bacon , H. Ko , D. Eyers , Twenty security considerations for cloud-supported internet of things, IEEE Internet Things J. 3 (June (3)) (2017) 269–284 .

[7] A .A . Osman , A . Rahim , U.H. Usi , User confidentiality protection in cloud com- puting using enhanced elliptic curve cryptography (ECC) algorithm, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 7 (11) (2017) 132–138

[8] S. Muthurajkumar , S. Ganapathy , M. Vijayalakshmi , A. Kannan , Secured tem- poral log management techniques for cloud, Procedia Comput. Sci. 46 (2015) 589–595 .

[9] T. Kalidoss , G. Sannasi , S. Lakshmanan , K. Kanagasabai , A. Kannan , Data anonymisation of vertically partitioned data using map reduce techniques on cloud, Int. J. Commun. Netw. Distrib. Syst. 20 (4) (2018) 519–531 .

[10] Lee, B.-H., Dewi, E. K., & Wajdi, M. F. (2018). *Data security in cloud computing using AES under HEROKU cloud. 2018*

[11] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems,

[12] 82, 395–411. doi:10.1016/j.future.2017.11.022

[13] Riad, K., & Ke, L. (2018). *Secure Storage and Retrieval of IoT Data Based on Private Information Retrieval. Wireless Communications and Mobile Computing, 2018, 1–8.* doi:10.1155/2018/5452463

[14] G. Wang , C. Liu , Y. Dong , P. Han , H. Pan , B. Fang , IDCrypt: a multi-user search- able symmetric encryption scheme for cloud applications, IEEE Access 6 (2018) 2908–2921 .

[15] Q. Zheng , X. Wang , M.K. Khan , S. Member , A lightweight authenticated en- cryption scheme based on chaotic SCML for railway cloud service, IEEE Access 6 (2018) 711–722 .

[16] S.J. Xiang , J.Y. He , Database authentication watermarking scheme in encrypted domain, IET Inf. Secur. 12 (1) (2018) .

[17] Wang, Toward performance and energy-efficient queries in three-tier wire- less sensor networks, in: ICPP 2018: , IEEE Access 6 (2018) 2895–2956 .

[18] H. Hammami , H. Brahmi , S. Ben Yahia , Secured outsourcing towards a cloud computing environment based on DNA cryptography, IET Inf. Secur. Netw. 2018 (Janua) (2018) .

[19] M. Kazim , L. Liu , S.Y. Zhu , A framework for orchestrating secure and dy- namic access of iot services in multi-cloud environments, IEEE Access 6 (2018) 58619–58633 .

[20] J. Shao , R. Lu , X. Lin , K. Liang , Secure bidirectional proxy re-encryption for cryptographic cloud storage, Pervasive Mob. Comput. 28 (2016) 113–121 .

[21] Q. Zheng , X. Wang , M.K. Khan , S. Member , A lightweight authenticated en- cryption scheme based on chaotic SCML for railway cloud service, IEEE Access 6 (2018) 711–722 .

[22] A .A . Osman , A . Rahim , U.H. Usi , User confidentiality protection in cloud com- puting using enhanced elliptic curve cryptography (ECC) algorithm, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 7 (11) (2017) 132–138 .

[23] P. Elumalaivasan , K. Kulothungan , S. Ganapathy , A. Kannan , Trust based cipher- text policy attribute based encryption techniques for decentralized disruption tolerant networks, Aust. J. Basic Appl. Sci. 10 (2) (2016) 18–26 .

[24] J. Fu , Y. Liu , H. Chao , B.K. Bhargava , Z. Zhang , Secure Data storage and search- ing for industrial iot by integrating fog computing and cloud computing, IEEE Trans. Ind. Inf. 14 (October (10)) (2018) 4519–4528 .

[25] X.L. Zheng , C.T. Huang , M. Matthews , Chinese remainder theorem based group key management, in: Association for Computing Machinery Proc. 45th Annual Southeast regional Conf. (ACMSE-07), Winston-Salem, North Carolina, USA, 2007, pp. 266–271 .

[26] W. Wang , P. Xu , L.T. Yang ,Secure data collection,storage and access in cloud-assisted IoT, IEEE Cloud Comput. 5 (July/August (4)) (2018) 77–88 .

[27] Guo, C., Zhuang, R., Su, C., Liu, C. Z., & Choo, K.-K. R. (2019). *Secure and Efficient K Nearest Neighbor Query over Encrypted Uncertain Data in Cloud-IoT Ecosystem. IEEE Internet of Things Journal, 1–1.* doi:10.1109/jiot.2019.2932775

[28] L. Jiang , D. Guo , Dynamic encrypted data sharing scheme based on condi- tional proxy broadcast re-encryption for cloud storage, IEEE Access 5 (2) (2019) 13336–13345

[29] Prabhu kavin, B., & Ganapathy, S. (2019). *A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. Computer Networks, 151, 181–190.* doi:10.1016/j.comnet.2019.01.032

[30] Chae, B. (Kevin). (2019). *The evolution of the Internet of Things (IoT): A computational text analysis. Telecommunications Policy, 101848.* doi:10.1016/j.telpol.2019.101848

[31] Xiong, J., Chen, L., Bhuiyan, M. Z. A., Cao, C., Wang, M., Luo, E., & Liu, X. (2019). *A secure data deletion scheme for IoT devices through key derivation encryption and data analysis. Future Generation Computer Systems.* doi:10.1016/j.future.2019.10.017

[32] Shin, D., Yun, K., Kim, J., Astillo, P. V., Kim, J.-N., & You, I. (2019). *A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks. IEEE Access, 7, 142531–142550.* doi:10.1109/access.2019.2943929