A Comprehensive Literature Review of Data Encryption Techniques in Cloud Computing and IoT Environment

Muhammad Sheraz Mehmood
Department of Computer Science
National Textile University
Faisalabad, Pakistan
sherazmehmood32@gmail.com

Muhammad Rehman Shahid
Department of Computer Science
National Textile University
Faisalabad, Pakistan
mrehman0892@gmail.com

Abid Jamil
Department of Computer Science
FAST - NUCES
Chiniot Faisalabad Campus , Pakistan
abid.jamil@nu.edu.pk

Rehan Ashraf
*Corresponding Author
Department of Computer Science
National Textile University
Faisalabad, Pakistan
rehan_ashraf94@yahoo.com

Toqeer Mahmood
Department of Computer Science
National Textile University
Faisalabad, Pakistan
toqeer.mahmood@yahoo.com

Aatif Mehmood
Department of Software Engineering
Foundation University Islamabad
Islamabad, Pakistan
atifmehmood369@gmail.com

***Abstract*—The internet of thing (IoT) is a network of interconnected physical devices, computer-based system, home-based application, automobiles and other things that are assigned with the unique IP address and devices may have the capability to share the data or information over networks without having any human to machine or human to human interaction. IoT devices generate a large volume of data is named Big data.Therefore, the concept of cloud computing was introduced to overcome storages issues on device. Cloud Computing is the latest emerging field which involves data processing and data storage to access remotely.However, the data on the internet is a risk. The IoT devices are generally small that consume less power and require less computational speed. As we know, the data encryption technique such as advanced encryption standard (AES), data encryption standard (DES) and triple advanced encryption standard (3DES) are complex algorithms.Therefore, these traditional encryption algorithms are not feasible for IoT devices. The issue mentioned above can be resolved by designing a lightweight encryption method to secure data transmission and communication in the IoT environment. The main objective of this research is to conduct a survey related to encryption techniques in cloud and IoT. This study summarize the encryption techniques, issues and variants, used for cloud and IoT. Furthermore, this study also presents the comparison of computational complexity of these techniques.**

***Index Terms*—Cloud Computing, IoT, Cryptography, Encryption, Decryption.**

I. Introduction

The internet of things (IoT) is a new technology, collection of billions of devices that produce big data. Day by day different types of data increase. Things could be everything like phones, wearable devices, cameras, sensors, vehicle. IoT is a concept of gathering the data, exchanging the data and processing the data with minimal human interference [1]. IoT changing our lives aspects to smartness like smart home, smart health, and smart cities. Smart things having controlled resources like limited battery and small size RAM. IoT devices required a unique Internet Protocol (IP) to connect with the internet. IoT based on physical objects which use sensors to collect data and shared the data with other objects over the internet [2]. IoT devices meant to produce big data. The growth of IoT devices is increasing day by day, which is reason Big data is emerging field. IoT based devices are generating different types of data that can be categorized into three types the Multi-structure, structure, and un-structure. To understand the concept of big data we must know V model [3]. The V model is based on Volume, Variety, and Velocity. Devices of IoT is generated an immense data which is difficult to manage. Few points are questionable; for example how to collect data for IoT devices and where to store, it is a difficult task to manage the privacy and security of the data in the IoT environment. Unfortunately, in IoT there a large number of applications and devices that are threatened; an intruder can quickly get the data, so that is the reason risk is higher in security and privacy parameters such as data integrity, confidentiality, authentication, access control, and others for IoT environment [5]. The prime attack on IoT devices is a loss of confidential information or modification of this information that is called confidentiality and Integrity. But encryption algorithms are more complex that consumes more energy of IoT based devices. That is the main reason, we need

978-1-7281-2334-9/19/$31.00 ©2019 IEEE

lightweight ciphers text for IoT to secure data transmission and communication. Consequently, we required to develop an efficient mechanism to secure connected devices on IoT form intruders and need to design a potent encryption algorithm for securing the data, also should be consuming less computational power. Currently, communication between IoT based devices become more convenient because of improvement in different fields such as RFID (Radio Frequency Identification), Mobile Communication, cloud computing, and WSN (Wireless Sensor Networks). Different sensors are embedded into objects and devices that are connected to IoT network. The data collected from different devices are analyzed to transfer important and useful information with the help of applications. IoT network is robust and time-saving of the platform which can determine precisely. The data can be used to predict the problems before it happened, identifying patterns, and making the best recommendations. The information is getting from connected devices on IoT network based on real-time that should be time and money-saving. The Generic model of IoT shows in figure 2.

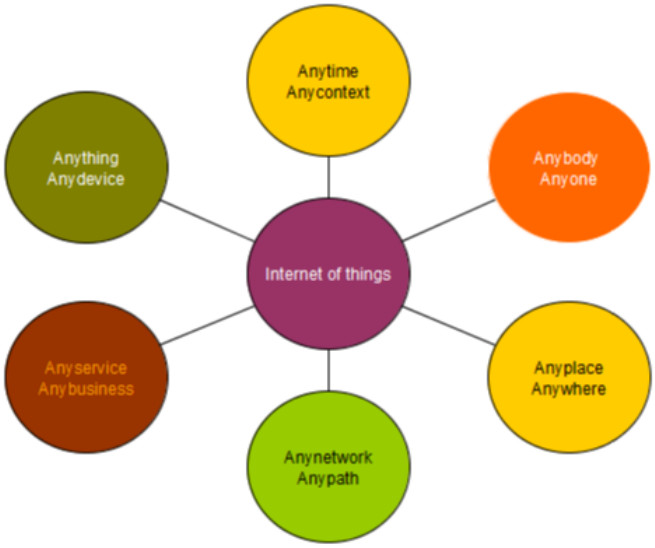

Fig. 1. Generic model of IoT

In IoT security of collected data on cloud networks is a big problem and managing the privacy of data also a difficult task. Unfortunately, lightweight devices and software are design in such a way that these devices and applications are failed to defend against security attacks [6]. The security and privacy of the data which is collected by IoT based devices are difficult to manage. Unfortunately, the mostly IoT based application and devices are not capable to handle the security attacks and that increased the security and privacy problem in IoT environments like data integrity, secrecy, authentication, access control and confidentiality [7]. The number of attacks on IoT based devices are increased day by day. According to a survey about 70% of the IoT devices are easy to hack. Thus, an efficient mechanism is required to secure the cloud data and IoT based devices. There is some main Security parameter in IoT are given below:

Confidentiality: The data transmission between the sender and receiver, human to machine, machine to machine, machine to human or human to human can be easily hacked by hacker. The security in IOT of End-to-End user is mandatory. The confidentiality can be achieved through encryption and decryption .

Compatibility: Currently, there is no international standard of compatibility for the tagging and monitoring equipment. The manufacturing companies of this equipment need to agree to a standard, such as Bluetooth, USB, etc.

Data Integrity: The data transmission between source and destination based on different stages, nobody allows to change the data at these stages. The intruder attacks on the data when it is traveling on the internet. That is why we need to apply some efficient methods to secure the data transmission, so the intruder cannot temper the data. Privacy/Security: With all this IoT data being transmitted, the risk of losing privacy increases. For instance, how well encrypted will the data be kept and transmitted with?

Authentication: Communicating entities should be able to authenticate the users. To ensure that the communication happens between the verified users.

II. Cloud Computing and IoT Integration

Over the last few years, cloud computing technology is building a powerful impact on advance smart services. The basic purpose of cloud computing is that gain access to the data and the information over the internet, therefore the hardware equipment can be eliminated or restricted. The IoT concept and cloud computing technologies have some similar major features. Internet of things structure can systems in different ways; many researchers have proposed different architectures in their style. Four types of interdependent systems required for IoT, Network Routers, Infrastructure of Network and Cloud. Cloud computing is a newly emerging field and allows to access the data and information anywhere and anytime thus without requiring the hardware [8]. IoT and Cloud computing both have some similar features such as storage, services, and application over the internet and consume less computational costs listed in TABLE 1.

A. Internet of Things

A Large number of devices are available including sensors, smartphones, vehicles, etc which interacts wirelessly. The Internet of things requires a system that is intelligent and capable of manage and filter data. The security alarms, mobile phones, GPS location, smart building, and sensors are examples of IoT.

B. Network Routers

Network routers are used to connect those designed things which are no able to communicate with the internet. In telecommunications, the term gateway refers to a piece of networking hardware that has the following meaning: In a communications network, a network node equipped for interfacing with another network that uses different protocols.

TABLE I
COMMON FEATURES OF IOT AND CLOUD COMPUTING

Feature	Internet of Things	Cloud Computing
Data storage on Internet	Yes	Yes
Services on Internet	Yes	Yes
Access of Application	Yes	Yes
Location-Free	Yes	Yes
Energy Efficiency	Yes	Yes
Computationally Capability	Yes	Yes

C. Infrastructure of Network

Internet is a worldwide connection of devices with IP networks. The infrastructure of the network is the combination of software and hardware resources of a whole network that enables network connectivity of the devices, communication, operations and management of an enterprise network. The structure of the network includes Routers, Switches, LAN Cards, and Wireless routers, which are used to control data traffic.

D. Cloud Server

Cloud computing is an Information Technology paradigm that enables all-over access to share configurable system resources whit minimal management effort. Cloud consist of large numbers of servers that are interconnected [10]. Cloud Set-up execute different types of applications are used to analyze collected data from different things to make accurate predictions, that structure use to endorse IoT atmosphere. In the cloud and IoT environment, the data of IoT devices can be access and store on cloud storage. Table no 1 explains the interactive feature of IoT and Cloud computing.

The rest of this work organized as follows: in section 2 describe the background of the cryptography algorithms used in IoT and cloud computing. Section 3 describe the related cryptography methods to this study. Section 4 describe the brief analysis of literature review. Section 5 briefly describe the conclusion.

III. BACKGROUND OF SECURITY METHODS

A. Cryptography

Cryptography is one of the most used techniques to build security. Cryptography considers a powerful technique and tool to secure the data. Cryptography with hash function is used to secure the computer password. The cryptography method SSL is also used to send secure emails. There is various aspect of cryptography confidentiality (only allowed person can access the data which has permission), integrity (the data cannot be modified or alter), authenticate (confirm the identity of sender and recipient). In cryptography the data is saved and transfer in such form that no one can understand except the sender and recipient. The third-party cannot understand or access this data. Encryption and Decryption are two main terms are used in cryptography. Encryption is a producer used to change plain text into chipper text. Vice versa decryption is used to change chipper text into plain text. Cryptography has two major types Symmetric and Asymmetric key cryptography.

B. Symmetric Cryptography

The symmetric cryptography algorithm used same key for data encryption/decryption. In technique the sender used a key to encrypt data and transfer to recipient, by using same key recipient decrypt data into plain text. The sender and recipient exchange the key by using secure medium to begin the discussion. There are different algorithms based on symmetric cryptography such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), Block Cipher, Caesar Cipher, and Stream Cipher.

C. Data Encryption Standard (DES)

The data encryption standard is a type of symmetric cryptography based on block cipher design by Horst Feistel. In DES algorithm same key used for encryption and decryption. DES encrypt data in blocks with the size of 64 bits. Input of 64 bits Plain text to DES generate the cipher text of 64 bits. The length of key in DES is 56 bits, however the algorithm is not used 8 of 64 bit for encryption.

D. Advance Encryption standard (AES)

Advance Encryption standard is popular and widely used encryption technique to secure information. AES method is much faster than DES and triple DES. AES algorithm is basic type of symmetric cryptography. The length of key is variable 128, 192 and 256 bits used for encryption.

E. Asymmetric Encryption

Asymmetric Cryptography is also named as public key encryption. In Asymmetric cryptography technique, two different public/private keys are used to encrypt/decrypt the data. Both sender and recipient have used their own public key and private key. Public/private keys have different purpose, public-key is used to encryption and private-key for decryption. The public-key is shared with other entity, whoever want to send the data can used public- key for encryption. The recipient used private-key for decryption, and private-key cannot be shared with others because its consider secret key. There are different types of algorithms are based on asymmetric cryptography such as ECC (Elliptic Curve Cryptography), and Diffie-Hellman, (RSA) Rivest - Shamir - Adleman.

F. Rivest - Shamir - Adleman (RSA) Cryptography

The RSA encryption technique is a type of asymmetric cryptography named for its developer Rivest - Shamir Adleman. The RSA technique is most commonly used for public key encryption. In this method, the data encrypt with public key which is shared with other users and private key use only for decrypt the data and its cannot be shared with others. In cloud computing the RSA use encrypt the data and stored into to cloud to secure data and avoid accessing by unauthorized users. The user request to access the data and after authenticating the user, the cloud provide allow to access it.

Detail	DES	AES	RSA	ECC
Developed date	1977	2000	1978	1985
Size of the key (bits)	56	128, 192 and 256	Minimum 1024	Max 1,024
Size of blocks (bits)	64	128	512	-
Technique	Symmetric	Symmetric	Asymmetric	Asymmetric
Key for Encryption Decryption	One key	One key	Different keys	Different keys
Scalability	Scale-able	-	-	-
Energy Consumption	Low	Low	high	Low
Encryption and Decryption	Fast	Fast	Slow	Fast
Implementation	Fast	Fast	Slow	Fast
Built-in Vulnerabilities	Brute Forced Attack, various cryptanalysis attacks and linear.	Brute Forced Attack	Brute Forced	Brute Forced Side-channel attack

G. Lightweight Cryptography

Internet of thing is collection of connected machines to machines and human to machines for communication and transfer data. In IoT smart devices consume less power and have low computational cost, that is way it is necessary to develop a lightweight cryptography to secure the data. Lightweight cryptography is a cryptographic used to implement in constrained environment such as sensors, healthcare devices, contactless smart cards and RFID tags and so on. For designing lightweight cryptography methods, both software and hardware specification are required to consider such as (how much time required for encryption and decryption), (how much energy required to consume), what RAM size occupied for compiles it. Lightweight cryptography refers to consume less computational cost its doesnt means that it will negotiate on the security.

H. Steganography

The word Steganography from Greek words steganos which meaning covered or concealed and the word graphein meaning is drawing or writing and that shows steganography meaning is covered writing. The Greeks was used this technique about 2000 years age to transfer the classified information. Steganography is the procedure to conceal the classified information within the other information. The file or data which is used to conceal classified information called the carrier. The information conceals within the carrier and the carrier modified in such way that looks similar to original. Images, audios and videos are the best carriers for the files. Basically, in steganography the is conceal no encrypt.

IV. Literature Review

Abdulatif Alabdulatif et al. [11] suggested security and privacy with any computational limitations overcome through a convenient data processing model that employs a single private server collaborating with a set of public servers within a cloud data center. Cryptography is used to avoid the Integrity attacks and stop the confidentiality outbreaks. Another novel approach for secure integration of Cloud was presented by Christos Stergiou et al. [12] named as a Secure Integration for both of IoT and Cloud Computing, based on Advance encryption Standard with its functionality. Decode-and-forward (DF) and amplify-and-forward (AF) model was used instead of truth relay. DF and AF provide strong key in AES which is beneficial security use of the encryption in integrate model. AES implementation needs less memory which makes it limited-memory environment. Ming Tao et al. [13] design ontology-based data semantic management and application model which is combination of the logical data and concepts of correlation based on smart home system. horizontal storage, vertical storage and decomposition, storage structures and relational database design based on ontology. Ruhul Amin et al. [14] developed a lightweight Authentication algorithm and protocol for improving security strength of IoT based devices in cloud computing environment. the author proposed AVISPA protocol tool and BAN logic model to proof security quality, length of the identity (user, server), password, random nonce, and message digest takes 128 bits each, and the communication protocol cost is 2816 bits. The proposed algorithm is evaluated check security strength on different criteria. User identification, Key sensitivity, session time, One-way hash function and logging are evaluation parameters. This study has some limitations which are addressed in this study. In 30, Lee et al. proposed the AES data security technique for cloud computing. Heroku cloud platform implemented and then they applied the AES encryption on the Heroku. The AES 128 bits key is used for data encryption and decryption. The AES characteristics are used such as rounds, key size, block size. The delay matric is used to evaluate the performance of the system. Jayant D. Bokefodea et al. [9] proposed an architecture to secure the cloud. There are two types of cryptography algorithm used Advanced Encryption Standard (AES) and Rivest, Shamir, and Adelman (RSA) applied mutually in this project. The Author used AES method through 128-bit key for encryption and decryption. Ping Li et al. [15] presented multiple-key homographic encryption technique to store data and hybrid structure scheme merging with dual decryption mechanisms. The authors measure the outcomes based on three aspects first is online attack by active users second is online attack by active server and third is outsider attack. First present a basic scheme based on multi-key fully homomorphic encryption (MK-FHE), then they propose an advanced scheme based on a hybrid structure by combining the double decryption mechanism and fully homomorphic encryption (FHE). The author also proves that these two multi-key privacy-preserving deep learning schemes over encrypted data are secure. Mehdi Bahrami et al. [16] suggested parallel encryption algorithm for securing electronic healthcare archives and introduce the broken glass for in case of emergency disaster retrieval for continuity and availability of system. The author measured results on bases of key generation, session key, continuity break-glass revocation, data recovery plan and session time. The study has various limitation which high cost of communication, complex and difficult structure of data recovery.

Fan wu, el at. [17] addresses the problem of authentication and communication of wearable devices. Wearable devices are smaller because of that have not enough storage. The authors proposed symmetric and asymmetric encryption algorithm for securing wearable devices. The author presented experiment with initialization, authentication, and paring. Which provides

Year	Authors	Techniques	Algorithm used	Structure Based	Key length	Rounds
2016	Christos Stergiou et al. [12]	Cryptography	AES & RSA	-	ASE 128,192, 256 bits & RSA 1024-4096 bits	AES 10, 12. 14 RSA 1
2016	Ruhul Amin et al. [14]	Cryptography	AES	One-Way Hash Function	128 bits	-
2016	Jayant D. Bokefode et al [9]	Cryptography	AES and RSA	-	128 bits	10
2016	Mehdi Bahrami et al. [16]	Data Privacy Method (DPM)	AES	Pseudorandom-Permutation (PRP)	128 bits	14
2016	Ming Tao et al. [13]	Security and privacy model	AES	Security tokes	128 bits	-
2016	Manish Kumar et al. [18]	Cryptographic	Dynamic key	-	128 bits	10
2017	Ping Li et al. [15]	Cryptographic	Double decryption mechanism	Hybrid Structure Scheme	-	-
2017	Abdulatif Alabdulatif et al. [11]	Cryptographic	lightweight-Homomorphic	Domingo-Ferrers	-	-
2017	Fan wu el at. [17]	Cryptographic	Symmetric-key algorithm	Hash Function & Exclusive or Operations	-	-
2017	Qinlong Huang et al. [19]	Cryptographic	symmetric encryption algorithm	hierarchical attribute-based encryption	-	-

more security. The author measured results on bases of time cost of cryptography, key, session key, time cost for (wearable device, cloud server, and smartphone) and communication cost. The proposed method cannot have applied to those wearable devices which do not have screens. Manish Kumar et al. [18] presented lightweight security model for IoT. With the information hiding technique, this proposed solution also provides security by using the cryptographic technique. For cryptography, a dynamic key is used. In the proposed solution they used 128-bit key that could not be accessed by brute force attack. It takes data of 8 bytes as an input and generates a fixed ciphertext of 8 bytes as output. It calculates sixteen subkeys of 8 bits from the 128-bit key. The results show that the model was able to detect all these slight changing and its ciphertext could not be decrypted. The result shows that system was able to detect minor changing. In [29], Qingchen Zhang et al. proposed possibilistic c-means algorithm (PCA) based on the homomorphic (BVG) encryption approach for securing the cloud computing big data. A novel scheme offered by Qinlong Huang et al. [19] to secure the data and efficient collaborate in cloud computing. The proposed system is based on hierarchical attribute-based encryption ABE. Attribute-based encryption applied to the encrypted user data and the encrypted data stored in cloud. In this paper [28], the authors proposed three data encryption techniques to secure the data for sharing over the internet. The authors implemented three different encryption techniques such as AES, DES, and RSA. The comparison of the implemented techniques is based on different factors such as size of the packet and the time of encryption and decryption time. In [31],Na Su et al. proposed DES technique based on the AES approach in IoT environment for securing the data. The AES technique is implemented in the four-general steps substitution, shifting-rows, mixing-columns and adding the round-key. In [32], Khan et al.

TABLE II
COMPARISON OF THE COMPUTATIONAL COMPLEXITY

Data Size (MB)	Encryption/ Decryption Time in (ms) [23]	Encryption/ Decryption Time in (ms) [11]
1	0.3/0.3	-
2	0.6/0.6	-
4	0.22/0.21	-
6	0.20/0.24	-
8	0.23/0.24	-
10	0.34/0.33	-
12	-	11.9418/5.0038
24	-	23.7261/11.0750
47	-	46.2950/23.594

Data Size (KB)	Time in (S) [24]	Time in (S) [25]	Time in (S) [26]	Time in (S) [27]
10	**	**	0.071465	0.0329
30	0.27	0.27	0.185454	0.0887
90	1.03	0.79	0.568465	0.1932
240	2.75	2.10	1.835408	0.5226

proposed Elliptic Curve Cryptography ECC technique for securing the data in cloud computing. The basic purpose of used ECC is that reducing the size of the key, because of the small key size helps minimize computational cost. ECC is applied for data encryption, decryption and, key-generation. The experiment results show that the computational cost of proposed ECC cryptography is less than the RSA. However, the decryption time of ECC is higher than the RSA.

V. CONCLUSION

The current study was attempt to explore the literature to describes lightweight cryptography techniques for cloud and IoT generated data. The Integration of IoT and cloud can reduce the computational cost because both have some features that can relate, including storage, services, applications over-internet and energy and computational efficiency. The

comparison of cryptography techniques in cloud computing and IoT environment is shown in Table 1. Furthermore, the comparison of the computational complexity of different algorithms is given in table 2 and table 3.The cryptography techniques can used to achieve authentication, data integrity and confidently by securing the data. Cloud computing is a newly emerging field that offers many opportunities for users to data processing and data storage out the devices. However, IoT devices generate extensive data so the security of the data is a challenging task. Cloud computing is considered as the best option for data storage of IoT devices. The different types of cryptography can be used to overcome this challenge. This study summerzie the literature to describe lightweight cryptography techniques to resolve security issues. This study can be extended to explore more literature by considering different application areas of cryptographic techniques.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 16451660, 2013.

[2] Z. H. Ali, H. A. Ali, and M. M. Badawy, Internet of Things (IoT): Definitions, Challenges and Recent Research Directions, Int. J. Comput. Appl., vol. 128, no. 1, pp. 3747, 2015.

[3] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. Ullah Khan, The rise of big data on cloud computing: Review and open research issues, Inf. Syst., vol. 47, pp. 98115, 2015.

[4] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. Ullah Khan, The rise of big data on cloud computing: Review and open research issues, Inf. Syst., vol. 47, pp. 98115, 2015

[5] T. Xu, J. B. Wendt, and M. Potkonjak, Security of IoT systems: Design challenges and opportunities, 2014 IEEE/ACM Int. Conf. Comput. Des., pp. 417423, 2014.

[6] A. Jamil, K. Asif, R. Ashraf, S. Mehmood, and G. Mustafa, A comprehensive study of cyber attacks & counter measures for web systems, Proc. 2nd Int. Conf. Futur. Networks Distrib. Syst. - ICFNDS 18, pp. 17, 2018.

[7] A. Balte, A. Kashid, and B. Patil, Security Issues in Internet of Things (IoT): A Survey, Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 4, p. 2277, 2015.

[8] B. Grobauer, T. Walloschek, and E. Stcker, Understanding cloud computing vulnerabilities, IEEE Secur. Priv., vol. 9, no. 2, pp. 5057, 2011.

[9] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption, Procedia Comput. Sci., vol. 89, pp. 4350, 2016.

[10] M. B. Jayalekshmi and S. H. Krishnaven, A Study on Data Storage Security Issues in Cloud Computing, Indian J. Sci. Technol., vol. 8, no. 24, pp. 128135, 2015.

[11] A. Alabdulatif, H. Kumarage, I. Khalil, and X. Yi, Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption, J. Comput. Syst. Sci., vol. 90, no. March, pp. 2845, 2017.

[12] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, Secure integration of IoT and Cloud Computing, Futur. Gener. Comput. Syst., vol. 78, pp. 964975, 2018.

[13] M. Tao, K. Ota, and M. Dong, Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes, Futur. Gener. Comput. Syst., vol. 76, pp. 528539, 2017.

[14] R. Amin, N. Kumar, G. P. Biswas, R. Iqbal, and V. Chang, A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment, Futur. Gener. Comput. Syst., 2016.

[15] P. Li et al., Multi-key privacy-preserving deep learning in cloud computing, Futur. Gener. Comput. Syst., vol. 74, pp. 7685, 2017.

[16] M. Bahrami, D. Li, and M. Singhal, An Efficient Parallel Implementation of a Light-weight Data Privacy Method for Mobile Cloud Users.

[17] F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, and J. Shen, A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server R, vol. 0, pp. 114, 2017.

[18] M. Kumar, S. Kumar, R. Budhiraja, M. K. Das, and S. Singh, Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach, Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016, no. 3, pp. 424428, 2017.

[19] Q. Huang, Y. Yang, and M. Shen, Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing, Futur. Gener. Comput. Syst., vol. 72, pp. 239249, 2017.

[20] N. K. Pareek, V. Patidar, and K. K. Sud, Discrete chaotic cryptography using external key, Phys. Lett. Sect. A Gen. At. Solid State Phys., vol. 309, no. 12, pp. 7582, 2003.

[21] N. K. Pareek, V. Patidar, and K. K. Sud, Cryptography using multiple one-dimensional chaotic maps, Commun. Nonlinear Sci. Numer. Simul., vol. 10, no. 7, pp. 715723, 2005.

[22] N. K. Preek, V. Patidar, K. K. Sud, Block cipher using 1D and 2D chaotic maps, International Journal of Information and Communication Technology 2 (3), 2010, pp. 244-259.

[23] J. Hur, D. Koo, Y. Shin, and K. Kang, Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage, IEEE Trans. Knowl. Data Eng., vol. 28, no. 11, pp. 31133125, 2016

[24] N.K. Pareek, V.Patidar, K.Sud, Discrete chaotic cryptography using external key, Physics Letters A 309(1), 2003, pp. 75-82.

[25] N. Pareek, V. Patidar, K. Sud, Cryptography using multiple onedimentional chaotic maps, Communications in Nonlinear Science and Numerical Simulation 10 (7), 2005, pp. 715-723.

[26] Manish Kumar, Sunil Kumar, Rajat Budhiraja, M.K. Das, Sanjeev Singh, A cryptographic model based on logistic map and a 3-D matrix, journal of information security and applications (2016), doi: 10.1016/j.jisa.2016.09.002

[27] M. Kumar, S. Kumar, R. Budhiraja, M. K. Das, and S. Singh, Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach, Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016, no. 3, pp. 424428, 2017.

[28] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, Secure integration of IoT and Cloud Computing, Futur. Gener. Comput. Syst., vol. 78, pp. 964975, 2018.

[29] Q. Zhang, L. T. Yang, A. Castiglione, Z. Chen, and P. Li, Secure weighted possibilistic c-means algorithm on cloud for clustering big data, Inf. Sci. (Ny)., vol. 479, pp. 515525, 2019.

[30] B. H. Lee, E. K. Dewi, and M. F. Wajdi, Data security in cloud computing using AES under HEROKU cloud, 2018 27th Wirel. Opt. Commun. Conf. WOCC 2018, pp. 15, 2018.

[31] Dey, Himel, Rifat Islam, and Hossain Arif. "An Integrated Model To Make Cloud Authentication And Multi-Tenancy More Secure." 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST). IEEE, 2019..

[32] Khan, I.A. and Qazi, R.Q., 2019. Data Security in Cloud Computing Using Elliptic Curve Cryptography. International Journal of Computing and Communication Networks, 1(1), pp.46-52.