iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XII **Month of publication:** December 2020

DOI: https://doi.org/10.22214/ijraset.2020.32639

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue XII Dec 2020- Available at www.ijraset.com

A Secure Data Communication Scheme Using RLE - ECC Cryptographic Algorithm in IoT Network

Samreen Aslam[1], Madhvi Arya[2]
[1]*Research Scholar of ECE Dept., SVIET, Banur, I.K. Gujral Punjab Technical University Punjab, India*
[2]*Asst. Prof. of ECE Dept., SVIET, Banur, I.K. Gujral Punjab Technical University Punjab, India*

Abstract: ***IoT is an emerging technology and is very popular as it increases the use of the internet. IoT offers ease of using the appliances and other objects with ease by utilizing embedded system. It offers communication between the humans and the machines through network of dispersed devices. It is being rapidly growing in various fields such as industries, digital services etc. Though it is complex but it has offered the ease in utilizing the technology. The main concern in IOT is the security of the data. It is required to use an effective prototype for security as highly advanced communication is being performed between this technology and the users. In this paper, a literature survey is presented to understand the work done in this field that showed a need of novel technology to be designed for providing the security to data. In the novel model, two-step security is provided to the data by using compression and encryption techniques. It enables the data to be protected and it can be receive without any alteration in the way. To this end, run length encoding and elliptical curve cryptography is utilized. Simulation of the results is performed in MATLAB software. The comparison is performed with the existing techniques in term of time consumed for processing. From the results, the existing system is observed to surpassed by proposed RLE2CC in various perspectives.***
Keywords**: *IoT, Security, run length encoding and elliptical curve cryptography.***

I. INTRODUCTION

IoT (Internet of things) was introduced in year 1999 by Kevin Ashton and it is highly preferable technology these days. To introduce the new term internet, he used the concept of radio frequency identification (RFID) [1]. When the term was introduced, it become one of the trending technologies and is used by all over the IT industry. As per the estimation of major companies, quantity of connected things in the world will have a thirtyfold increase between 2009 and 2020, but in 2020 there will be large number of things which are connected to the internet.

Due to the massive use of IoT based applications in the market, various security problems occurred sharply. These problems need to be counted because things and devices are becoming a part of internet infrastructure. When the device is connected with the internet, then these issues become an important part. Sometimes these security flaws are diminished by the hackers, and even they are wrongly used in uncontrolled environments with billions of IoT devices [2]. To control this, IoT will increase the potential attacks for cybercriminals and hackers. A theory stated by Hewlett Packard [3] introduced that 70% of the majorly used Internet of things devices consists of dangerous vulnerabilities.

Thus, IoT devices are in danger due to its design which lacking some security features, for example, insufficient authentication, insecure communication medium, and authorization configurations. When IoT is used everywhere in the industry or by the individuals then all the industries should be concerned. To exchange and influence new potentials, cross-linking objects are presented. New concerning information and data protection will lead to plenty of new potential risks. Moreover, these improper securities create resistance to select the technique of IoT by companies and individuals. Some of the challenges and issues should be mentioned while providing the proper training to the developers and designers to add the security issues into the IoT and encouraging the users to use the special IoT security features that are developed into the devices [2].

As per the increasing number of devices that are connected through IoT, are having more security issues and multiple cases are increasing as well as many of these security issues disturb the entire system [4]. Due to the designed system of IoT technologies, conventional security methods are not straightforwardly implemented because these restricted powers and a huge number of connected devices increase the scalability issues and heterogeneity [5]. Sometimes the safety and security of these systems can be in high danger and sometime it can be unpredictable and predictable, and sometime its consideration should be difficult to bring the system's elasticity.

As per the research [6], there are four types of the data security issue: integrity, authenticity, confidentiality and data availability. These type issues should be fixed by implementing some security measures.

To implement the IoT effectively, security requirements play a very significant role. According to the security principle, the designs of the management system and security solutions are developed. To accomplish the IoT based security system there is some important requirement which is mention below [7-11].

A. Availability
B. Accountability
C. Auditing
D. Authentication and Authorization
E. Access control
F. Privacy
G. Confidentiality
H. Integrity
I. Non-repudiation

IoT required the advance and up-to-date prototype for protecting security which takes security problems for the whole perspective including the latest customers and their interaction with this technology. It has thus became one of the most attractive research field and number of researchers are carried out to provide security in the IoT systems. Some of the existing works are discussed in the next section:

II. LITERATURE REVIEW

As defined in above section, it is problematic to give security to the IoT systems and also is the major concern. To solve this problem, a lot of algorithms are being developed for giving the security to the data. Some of these are reviewed below:

The paper [12] sets forward an advanced encryption/decryption algorithm that was based on the Binary-Bit sequence, ASCII and further uses the XOR operation.

In paper [13], the detailed information about the security challenges on IoT devices and mobile phones were mentioned. Also, the various security attacks and their prevention methods with their detailed advantages and disadvantages after the planned algorithms were presented.

The paper [14] defined a layout of AES-GCM core that provided the privacy by Counter mode of block cipher AES, and it also gave authenticity and integrity by GHASH. AES encryption supported two key dimensions of key length 128 and 256 bit.

In proposed paper [15], a hybrid and authenticated algorithm was proposed for communication and stored the information in the cloud.

The planned algorithm allows the edge device to encrypt the information generated by the Advanced Encryption Standard (AES) before transmitted to the cloud. RSA cryptosystem had encrypted the AES.

Symmetric cryptography and a schematic consisting of Asymmetric was defined in [16] to protect the message between the devices in an IoT system.

The author in [17] had proposed a customized encrypted algorithm and an authenticated scheme for securely transmitted the information. This algorithm was a variation of AES and developed the new protocol for key formation.

A novel designed was proposed in [18] that was a hybrid encryption algorithm that had been directed to reduce security problems and less computational complexity and enhancing encryption speed.

The author in [19] had proposed the efficient architecture of security management servers that improved the safety and security of IoT devices in the environment of the IoT.

The author had invented a multi-hop routing protocol in paper [20] that allowed safe communication in the IoT devices.

In paper [21], the pros and cons of the IoT had been surveyed and also the advance approaches that ensured the fundamental and essential security requisites and secured interlinked of IoT, along with the changed rolling and scope for the work in this field in the coming future.

In this, author has utilized two encryption techniques, namely, AES and NTRU to achieve security. AES is used for key generation and encryption is provided by NTRU system. This system gives better results; however, it can be upgraded further to attain more efficient results.

III.PRESENT WORK

As reviewed in above section, many researchers have performed different studies to maintain the security in the IoT system. One such approach is reviewed [21] in which author has utilized two encryption techniques, namely, AES and NTRU to achieve security. This system gives better results; however, it can be upgraded as NTRU technique may not be feasible due to its complexity. Moreover, it is an open source algorithm of encryption in which, updations are made on the daily basis. Until, the stable version of NTRU is designed, implementing it in the system may not be good decision. Thus, there is need of developing of Security model for IOT which must be more trustable and stable and better encryption algorithms must be used to provide more security.

Thus, the need of novel approach is fulfilled by proposing a novel model to offer security in IoT. In the proposed work, key generation is carried out by using AES. This approach remains same in the novel design as AES is an efficient approach.

Further, Multi-level encryption is introduced in the security model that includes encoding and encryption of data retrieved through IoT. After generation of the key, firstly, the data is secured by applying Run length Encoding (RLE) technique.

RLE is the lossless compression technique which helps in transmitting the same data i.e. no data loss will be experienced. This is one of the approach how data is given security.

Further, to the compressed data, Elliptic curve cryptography (ECC) encryption algorithm is applied. ECC is used for encryption due to its fast and effective performance. Also, ECC is a secure method of encryption.

Thus, in the proposed model, two level securities is provided by applying compression and encryption mechanisms.

Besides this, in the previous work [21] author analyzed the performance of the algorithm by using only one parameter i.e. Speed of Implementation Algorithm.

In the novel approach three different parameters are introduced to determine the efficiency of the proposed work. These three parameters are:

A. Key size
B. Compression Ratio
C. Data Size

The flowchart of the proposed system is shown below:

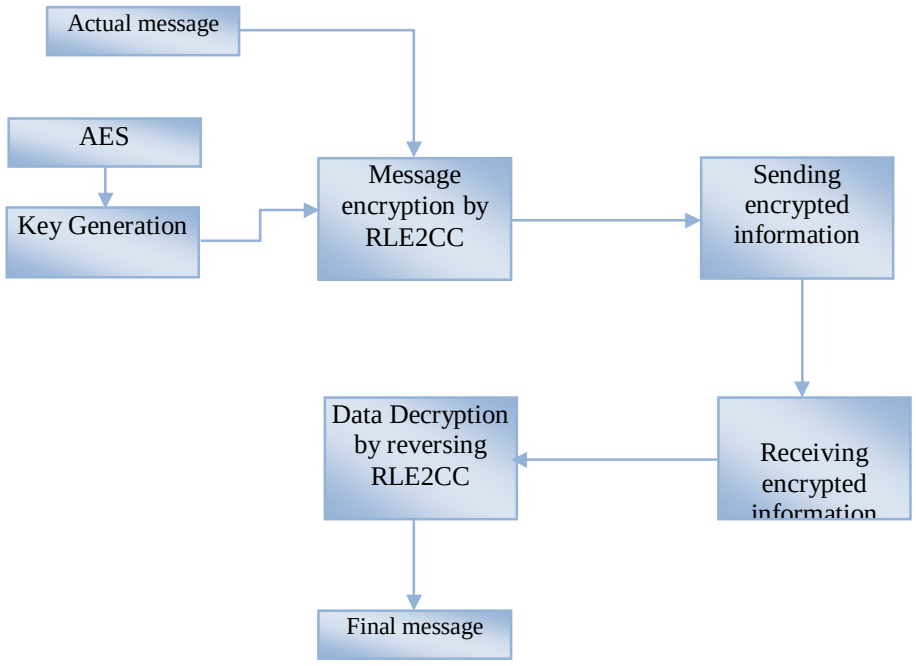


Figure 1: Flow chart of proposed system

The performance of this proposed system is then analyzed in terms of various parameters to demonstrate its performance efficiency. The obtained results are shown in next section

IV. RESULTS AND DISCUSSIONS

This section discusses the results obtained after implementation of the proposed model. The proposed model aimed to offer security to the data available in IoT by using encryption of the data and eventually compressing it in order to provide double security. The simulation of the model is performed in MATLAB software using RLE and ECC techniques. The results are obtained for the model and are validated by performing performance analysis with the existing data security techniques such as HAN and AES. As the proposed technique used run length encoding (RLE) and Ellptical curve Cryptography (ECC), it is named as RLE2CC. The model is tested for different parameters such as time taken to secure the given data, data size before and after compression, standard deviation and variation.

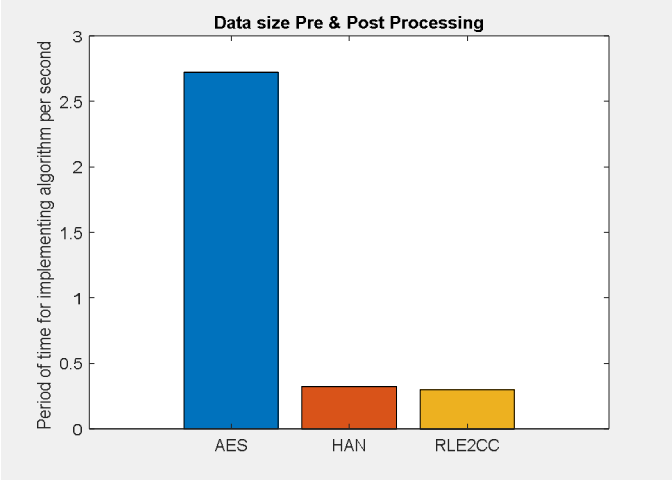


Figure 2: Period time for implementing algorithm per second

Figure 2 demonstrates the results in a graphical form and the bar graph illustrates the period time utilized by the algorithms while implementing algorithm. The time is measured in seconds. The comparison is shown between three algorithms namely, AES, HAN and RLE2CC. It is observed from the graph that AES technique took the highest time for its implementation and it accounted to nearly 2.7 seconds. However, the proposed RLE2CC and existing HAN techniques showed almost similar time which is very less as compared to that of AES approach. The time consumes by HAN and RLE2CC accounted to approximately 0.4 and 0.3 respectively.

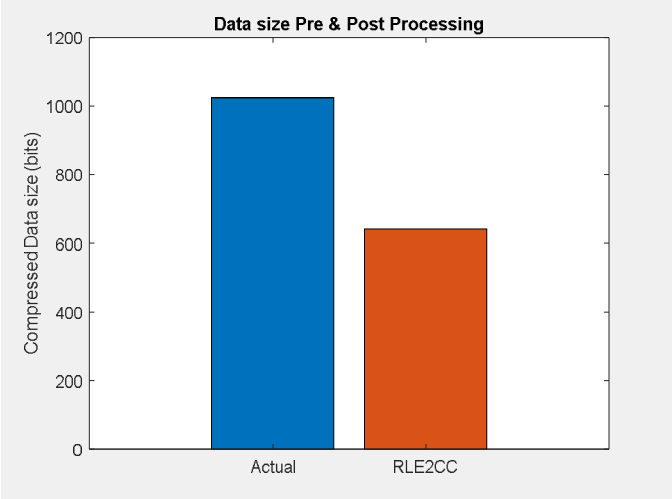


Figure 3: Comparison of compressed and actual data size

Figure 3 demonstrates the data size before and after applying the proposed model on the specific data. A significant difference is observed as the actual data constituted to nearly 1000 bits whereas after compression the size becomes approximately 600 bits. The size is reduced by almost 400 bits that illustrated that the proposed technique is capable of providing security to the original data..

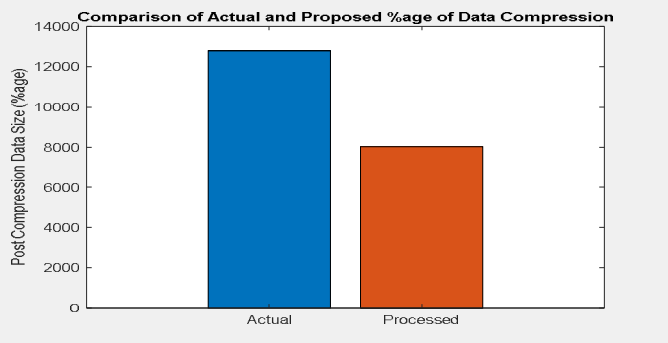


Figure 4: Comparison of post compression data size.

The comparison of the percentage of the actual and the compressed data is delineated in figure 4. It can be seen from the shown graph that after compression of the data the size is further reduced by processing the data. The actual data size as early 13000 which reduced to 8000. This graph presented that the proposed model has the capability to reduce the data size to a great extent that increases the security of data in IoT.

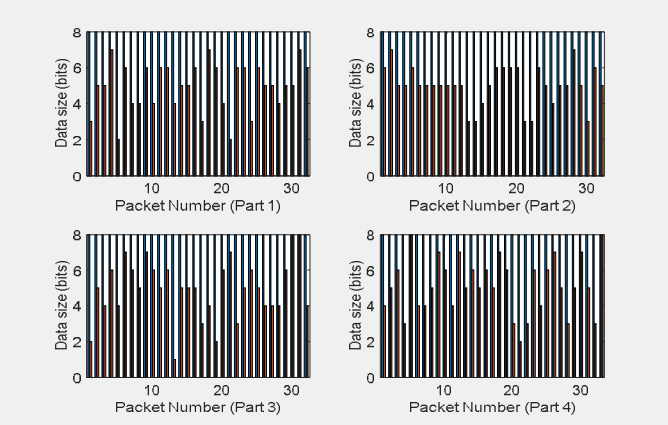


Figure 5: Representation for different packet numbers with respect to actual data size

As it is known that the data is transmitted from the source to destination in the form of packets, the performance of the packets is determined with respect to the compressed data. Each packet delivers a specific amount of data. When the proposed model was implemented, it processed the data in the packets and compresses the data that results in reducing he data size to a great extent. The figure 5 shows the graph that illustrates relation of four different scenarios for certain number of packets with respect to data size in the form of percentage.

Similarly, in figure 6, the graph is demonstrating the compressed data for different number and packets. It also gives four scenarios. The data size is reduced after the compression of the data.

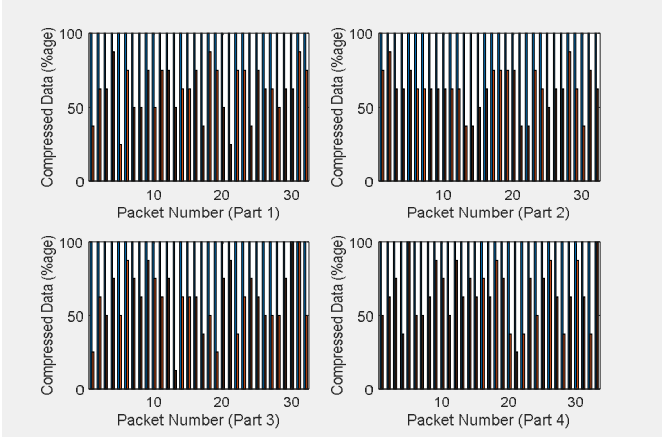


Figure 6: Representation of packets with respect to compressed data

Further, the parameters of the proposed work, namely, standard variation and variance are computed and the results are presented in a graphical view. Figure 7 delineates the parameter values on y axis and the parameters on the x axis. The close examination of the graph reveals that the standard deviation is less that the variance and it accounted to 1.23 approximately. The variance for the proposed work is 1.52.

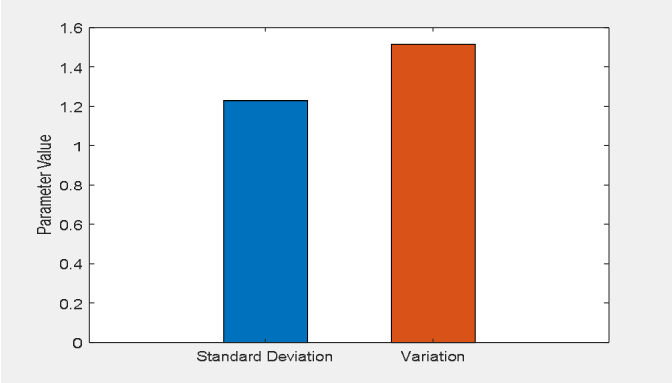


Figure 7: Variation and standard deviation for proposed technique

Overall, it is clear from the results that the proposed work is effective in terms of providing the data security as it used the cryptography method to encrypt the data and also compresses the data for its double security.

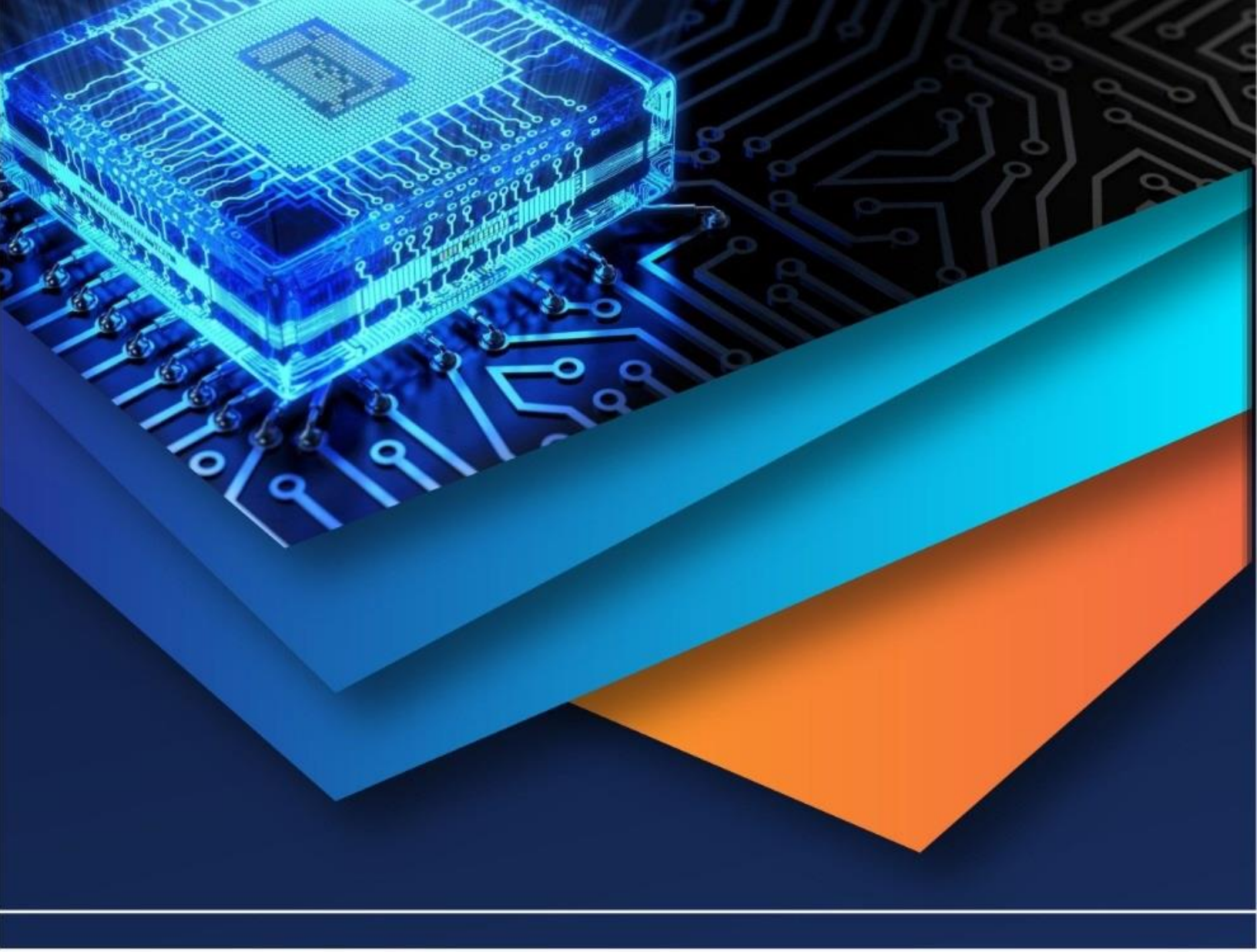
V. CONCLUSION

In this paper, the main aim of research is to develop an algorithm that can offer security to the data that is transmitted over IoT. A review is performed to know the existing techniques that have already been designed to this end. It is observed that techniques such as AES, HAN are being used, however the several limitation lead to design a novel model using two techniques. Thus, the proposed work is designed which offer two times security as data is compressed and then it is encrypted. For this purpose, Run length encoding is used for data compression and Elliptical curve cryptography is utilized for data encryption. The simulation is performed in MATLAB software where the model is implemented and the results are obtained and a comparative performance is performed with the existing techniques. To evaluate the performance, period time is considered for each algorithm that showed that proposed RLE2CC consumed less time than other techniques. The comparison with the size of actual and compressed data demonstrated a huge difference between the sizes. The processed data differs from the actual data in terms of data size and originality. Eventually, the standard deviation and the variation of the RLE2CC accounted to 1.23 and 1.51 respectively which suggested the effective performance of proposed strategy to offer security.

REFERENCES

[1] K. Ashton, "That 'Internet of Things'," 22 June 2009. [Online]. Available: http://www.rfidjournal.com/articles/view?4986. [Accessed 02 April 2015].
[2] Abomhara, M., Køien, G.M.: Security and privacy in the Internet of Things: current status and open issues. In: International Conference on Privacy and Security in Mobile Systems (PRISMS). IEEE (2014)
[3] Gen, H.P.-C.S.A. Controllers, R.: Hewlett-Packard Enterprise Development LP. Citeseer (2015)
[4] Jing, Q., et al.: Security of the internet of things: perspectives and challenges. Wirel. Netw. 20(8), 2481–2501 (2014)
[5] Sicari, S., et al., "Security, privacy and trust in Internet of Things: the road ahead", Comput. Netw. 76, 146–164 (2015)
[6] Suo, H., et al:. Security and privacy in mobile cloud computing. In: 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE (2013)
[7] Hui Suoa, Jiafu Wan, Caifeng Zoua, Jianqi Liu, " Security in the In-ternet of Things: A Review", Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), Hangzhou, China, pp. 648- 651, 23-25 March 2012.
[8] M.U. Farooq, Muhammad Waseem, Sadia Mazhar, "A Review on Internet of Things (IoT)", International Journal of Computer Applica-tions, vol. 113, no. 1, pp1-7, 2015.
[9] Mohamed Abomhara and Geir M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks", Journal of Cyber Security, vol. 4,pp. 65-88, 2015.
[10] Otmane El Mouaatamid, Mohammed Lahmer, Mostafa Belkasmi, "Internet of Things Security: Layered Classification of Attacks and Possible Countermeasures, Electronic Journal of Information Tech-nology, Issue 9, pp. 24-37, 2016.
[11] Rolf H. Weber, "Accountability in the Internet of Things", Computer law & security review, vol. 27, no. 4, pp. 133-138, 2011
[12] I. Hussain, M. C. Negi and N. Pandey, "Proposing an Encryption/ Decryption Scheme for IoT Communications using Binary-bit Sequence and Multistage Encryption," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2018, pp. 709-713

[13] S. Chaudhry, "An Encryption-based Secure Framework for Data Transmission in IoT," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2018, pp. 743-747.
[14] B. Sung, K. Kim and K. Shin, "An AES-GCM authenticated encryption crypto-core for IoT security," 2018 International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, 2018, pp. 1-3.
[15] Y. Chandu, K. S. R. Kumar, N. V. Prabhukhanolkar, A. N. Anish and S. Rawal, "Design and implementation of hybrid encryption for security of IOT data," 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), Bangalore, 2017, pp. 1228-1231.
[16] M. S. Henriques and N. K. Vernekar, "Using symmetric and asymmetric cryptography to secure communication between devices in IoT," 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, 2017, pp. 1-4
[17] B. Daddala, H. Wang and A. Y. Javaid, "Design and implementation of a customized encryption algorithm for authentication and secure communication between devices," 2017 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, 2017, pp. 258-262
[18] A. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, 2017, pp. 1-5.
[19] S. Yoon and J. Kim, "Remote security management server for IoT devices," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 1162-1164
[20] P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 428-432
[21] S. Narang, T. Nalwa, T. Choudhury and N. Kashyap, "An efficient method for security measurement in internet of things," 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT), Chennai, India, 2018, pp. 319-323



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY