ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.5, 2903–2911
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.5.52

EFFICIENT MATHEMATICAL ENCRYPTION (EME) MODEL FOR SECURING IOT DEVICE COMMUNICATION

M. SUNDARRAJAN[1] AND A. E. NARAYANAN

ABSTRACT. IOT rebellion plays a vital role in the developments of wireless technology leading to an exponential growth in device connectivity. Embedded devices will help in processing and managing of enormous quantity of data and aiding in its transmission in the network. The significant area in IoT field is the security and safety of data transmission. Abundant algorithms supporting encryption are been suggested to handle secured data transmission in IoT environment. TEA (Tiny Encryption Algorithm) is the majorly known algorithm with less utilization of memory and easy handling of both hardware and software system. But there is one disadvantage of this algorithm is that it will utilize the same key in all the encrypting levels leading to reduced security approach. The time acquired for text for encrypting and decrypting process is also very high denoting less IoT network efficiency in spite of utilizing embedded devices. In our paper we have suggested an approach named EME (Efficient Mathematical Encryption) providing improvedsecurity text files transmission in the IoT environment with the help of introduction of additional keys which is added dynamically for every round of encrypting procedure. We have experimentally verified our suggested approach to check the effect of avalanche, encrypting and decrypting EME time in IoT environment along with embedded devices. The results prove that our EME algorithm is very much secured and proficient in comparison with the current encrypting algorithms.

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 68P25, 94A60.

Key words and phrases. Encryption, Decryption, Time, EME, Transmission, Symmetric Encryption, Security, Efficiency, Key confusions.

1. INTRODUCTION

IoT embraces lots of device connections involving data communication and data computing. Enormous data communication will happen between these devices for every second. IoT applications such as portable health devices, connected vehicles etc. will require secured information transmission which is an important concern in the emerging technological field. There are various hackers and invaders whose count is keep on increasing thereby challenging our concern of security and safety in the network. In the past years various cryptographic algorithms are used for secured data transmission. It is very popular because of its techniques utilized to establish and manage secret distribution of keys. It will be useless in case of poor maintenance. It is classified in to symmetric and asymmetric algorithm. Same key is utilized for encrypting and decrypting procedure in the case of symmetric algorithm. Here block ciphers and stream ciphers are also used. But in the case of asymmetric key algorithm public and private key is been utilized for encrypting and decrypting procedure. Every IoT device will have a unique capability. But for all the significant requirements is security, safety, efficiencyand light weight. Time taken for complete processing should be less and performance should be higher. The algorithm used should be with less complexity and less overhead. In our paper, we have proposed an algorithm named EFFICIENTEME ENCRYPTION (EME) by improvising the security features of TEA algorithm. Here we introduce dynamic and multiple keys which will be added in various encrypting phases for improve security of our transmission algorithm. At the execution time, the values of the keys are altered and cannot do pre-computation. EME will take only less time for both encryption and decryption in comparison with TEA and thereby providing more security and efficiency in IoT networking environment. We have provided all our research works in the literature survey session, brief explanation of various current encrypting methodologies for secured data transmission, detailed explanation to EME, experimental results are also explained clearly and a proper conclusion is given along with future works as well.

2. Related Works

Here we have discussed about various research works involving data transmission in IoT specifically how the algorithms are designed and their implementation procedures. In [1], they have proposed a RUASN scheme with a two factor perception. It possesses various advantages over the current attacks in the network and works well in efficient low consumption. They have proven an idea that session key can be gained by way of controlling the concededsensor node and with the aid of collusion attack when user in need for session establishment with legal node. For improvising the collusion attack's resistance and to resolve the security problems of their scheme they present two approaches. One approach is to enhance RUASN improvement scheme and the other utilizing the hardware security and safety module. In [2], they have discussed about the power of quantum computers on security related researches in IoT technology. From these research studies comparison is made with the important attributes. The security of the IoT environment ranges board and chip phase, software layer security, protocol security, network security, susceptible algorithm of cryptography, social engineering and malwares like Trojan horse, ransomware etc. They also discussed about the difficulties faced to identify the vulnerabilities and risks available in IoT environment.

In [3], they design a fog computing architecture completely basedon the parameter 'QoS'. They also provide a cloud-IoT solution which is distributed in nature. Here optimal distribution happens among various fog nodes. VM's will take care of IoT processing which is located within the devices at the edge. They suggest a fog computing model for EME formulation. They present a QoS metrics system with performance analysis. In [4], they present a document mentioning the limitations and applicability of the current IP related security protocols in wireless networking environment. The complete analysis of these protocols is conversed related to taxonomy which is mainly focused on key distributed mechanism. In [5], they make a study on significant outage performance for network communication in wireless mode under collusion of eavesdropper in which security at physical layer is embraced to counteract such attacks. Initially they perform an analysis on secrecy outage of non-colluding case for which eavesdroppers will operate independently. Observations are combined by eavesdroppersto decode message, keyhole counter integral, Laplace transform techniques

and Cauchy integral theorem for dangerous M-colluding scenario are adopted to handle multi-fold convolution problem and therefore analytical determination of outage probability is done. The system is experimentally verified to prove their theoretical achievements.

In [6], they have designed a fog computing based new architecture related on QoS parameters. They present an optimal fog nodes distribution based solution for IoT cloud. The facilitation of VMs located in the edge devices is done by the mini clouds for handling IoT traffic. A perfect EME formulation for their suggested model and performance analysis is proposed in terms of QoS metrics. In [7], they suggest a framework offering secured communication system among internet host and IoT nodes by connecting an encryption system with public key cryptography. They also provide a distinct key generation and novel generation system to provide security to entire communication system. After the simulation the results shows that its performance is far better than the existing system. In [8], this paper mainly focuses on the compressive sensing methodology based on the security issue and they suggest an effective and efficient lightweight scheme with full security which will handle the challenges faced previously. For experimental verification, collection of data is done from real sensors present in the research lab named Intel Berkeley.

In [9], here it is nothing but an article providing a detailed survey on post quantum IoT systems which are the systems secured from computing quantum attacks. Reviewing of cryptosystems of post quantum and initiatives are done and analysis of appropriate IoT challenges and architectures are done. The expectations of future trends are also indicated here. Finally they provide essential guidelines for post quantum IoT security and future version of it. In [10], they have suggested an ECC related biometrics based scheme of authentication. For proving the security strength of their scheme both informal and formal analysis of the scheme is carried out. To ensure that their scheme is against potential threat they perform simulation with AVISPA. They have also compared their suggested scheme with computation cost parameter and security features and the superiority of the scheme is also proven with other related schemes.

3. Proposed Approach

In our proposed approach we are using EME model for both encryption and decryption mechanism. There are two phases in our module. One is the sender side and the other is the receiver side. The source files can be of any file format like image file or a document file or spreadsheet file or presentation file etc. All the files are considered in our model for encrypting phase. We also make a check to confirm whether the source file is a text file or not since EME can directly proceed with the encryption mechanism else the file should undergo binary conversion (0's and 1's) and then the EME Formula will proceed further. With the aid of this encryption algorithm source file to cipher text conversion will happen. Now the decryption phase starts when the cipher text successfully travels through IoT networking environment. Here the conversion of cipher text to plain text will happen. The converted file can be either binary or direct source file based on its type. Secret key is utilized for binary file conversion and it will be share between sender and receiver side.

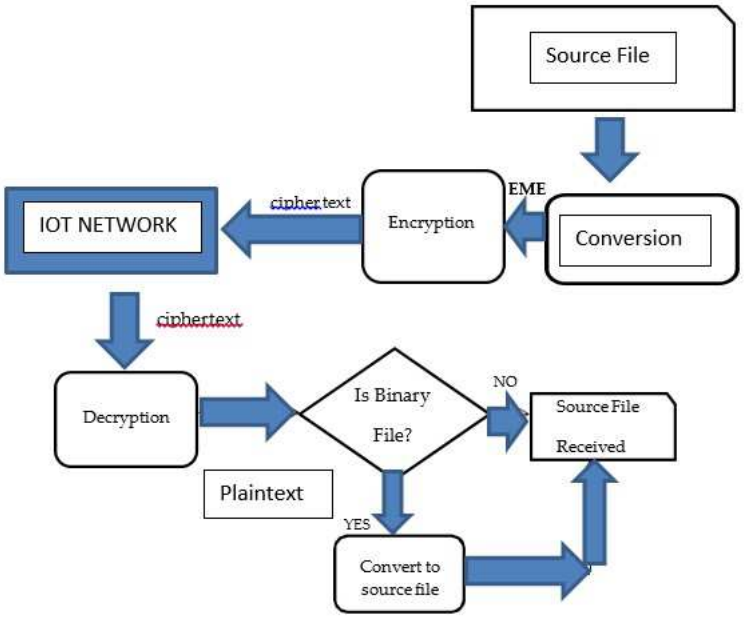

Fig. 1 EME Architecture

In fig.1, source file of any type including document, images, presentations, spreadsheet etc., is sent to the EME algorithm along with a conversion where the received source file is checked whether it is a text file or not. If not the file is converted to binary form and then undergo EME process. During the conversion

a secret key is shared between sender and the receiver side. Once the cipher text is generated from the EME phase it can be shared through IoT networking environment without any security breach. Now for the receiver to receive it back we have to undergo decryption phase. Here comes the EME decrypting algorithm where the cipher text will be converted to plain text. In case of binary conversion the process will happen and then the source file will be received at the receiver end. This is how our EME approach will add security to IoT networking environment without any security breaches as we mentioned in equations (3.1) and (3.2).

Encryption:

$$C = K^e(modd) + RN \tag{3.1}$$

Decryption:

$$K - C^d(modd) + RN \tag{3.2}$$

Here, C - Cipher text, K - Key, d - Number of devices and RN - Random Numbers.

4. Experimental Results

We have experimentally verified our suggested idea to compare our model's behavior over the current model, TEA that supports IoT security. We utilize secret key for every module undergoing encryption and decryption which is shared between both the sender and the receiver. Based on the key size and the bit changes in the cipher text we record the behavior through graphical representation.

Fig.2 depicts the alterations in the key and the corresponding alterations in the cipher text. The block size is of 64 bits. The graph is plotted between key size from '0' to '128' bits and the cipher text's bit changes from '0' to '15' bits. The red markings are mentioned for TEA module and the blue marking is mentioned for our suggested EME module. From the graph it is very clear that for 64 bit block, a change is noted in one bit of the key applicable for various key sizes and the same change is recorded in the cipher text for both TEA and EME. For the key size '48' the cipher text created by the TEA's change is less compared to the EME's cipher text's changes. For key size '128' also the same behavior is

recorded. Thus from this graph we can conclude that for a key size the change in the TEA created cipher text is very less compared to the EME created cipher text.

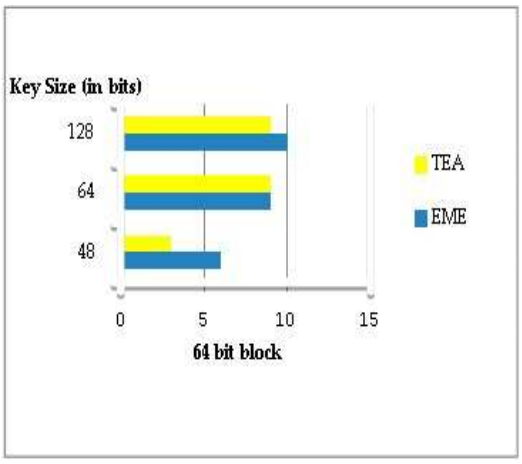

Fig.2 Change in key size and the corresponding change in cipher text for a 64-bit block.

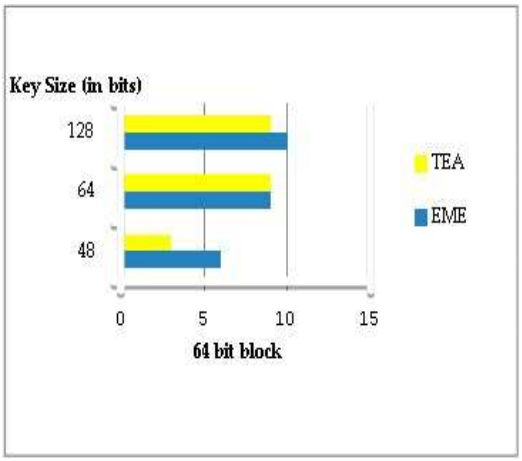

Fig.3 One-bit change in plaintext corresponding change in cipher text for 64-bit block.

In Fig.3, the graph is plotted between key size measured in bits and the change in bits in the created cipher text. The changes are recorded with one bit changes. The comparison is made in between both TEA and EME. The key size value starts from '0' to '128' bit size and the created cipher text's bit change values are plotted from '0' to '10' bit size. It is very much clear that when a plaintext's bit is change with one bit variation then the generation of cipher text with the

help of our suggested EME model happens which depicts more alterations when compared to the cipher text created by TEA. The variations can be easily seen for all the values from '0' to '128' bit key size. Thus from our suggested approach more efficiency can recorded from EME and it is very much secure in comparison with other previously suggested models when a text file has to be transmitted between embedded IoT devices. All the security needs for this approach is met to our satisfaction.

5. Conclusion

Previously suggested secured models such as TEA along with its versions like XTEA and XXTEA had better performance constraints in terms of encryption methodology and decrypting methodology. But our suggested EME module behaves in a same way as the previous modules but when experimentally verified its performance is much better compared with other modules. EME will take only less time for both encryption and decryption in comparison with TEA and thereby providing more security and efficiency in IoT networking environment. It also creates more key confusions than TEA. Further encryption of the compressed file will create even more security to EME algorithm. In our paper we have presented our idea from related works in detail, detailed explanation of our EME algorithmic structure and experimental verification by graphical charts plotting for parameters key size bits and cipher text bits and the obtained results proves that EME is far more effective with security satisfying needs compared with other models.

References

[1] L. Chi, L. Hu, H. Li, J. Chu: *Analysis and improvement of a robust user authentication framework for ubiquitous sensor networks*, International Journal of Distributed Sensor Networks, **10**(3) (2014).

[2] M.A. Sadeeq, S.R. Zeebaree, R. Qashi, S.H. Ahmed, K. Jacksi: *Internet of Things security: a survey*, International Conference on Advanced Science and Engineering (ICOASE), IEEE, 2018, 162–166.

[3] P. Maiti, J. Shukla, B. Sahoo, A. K. Turuk: *Mathematical Model of Fog Computing Architecture for IoT Micro-Services*, International Conference on Emerging Technologies in Data Mining and Information Security (IEMIS2018), Kolkata, West Bengal. India, 2018.

[4] K.T. NGUYEN, M. LAURENT, N. OUALHA: *Survey on secure communication protocols for the Internet of Things*, Ad Hoc Networks, **32** (2015), 17-31.

[5] Y. ZHANG, Y. SHEN, H. WANG, J. YONG, X. JIANG: *On secure wireless communications for IoT under eavesdropper collusion*, IEEE Transactions on Automation Science and Engineering, **13**(3) (2015), 1281-1293.

[6] P. MAITI, J. SHUKLA, B. SAHOO, A.K. TURUK: *Mathematical modeling of QoS-aware fog computing architecture for IoT services*, Emerging Technologies in Data Mining and Information Security, Advances in Intelligent Systems and Computing, **814** (2019), 13-21.

[7] N. FATHIMA, R. BANU, G.F. ALI AHAMMED: *Modeling of Secure Communication in Internet-of-Things for Resisting Potential Intrusion*, Computational Statistics and Mathematical Modeling Methods in Intelligent Systems, Advances in Intelligent Systems and Computing, **1047** (2019), 389-398.

[8] A. AZIZ, K. SINGH: *Lightweight Security Scheme for Internet of Things*, Wireless Personal Communications, **104**(2) (2019), 577-593.

[9] T.M. FERNÁNDEZ-CARAMÉS: *From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things*, IEEE Internet of Things Journal, (2019).

[10] P.K. DHILLON, S. KALRA: *Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things*, Multimedia Tools and Applications, **78**(16) (2019), 22199-22222.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
PERIYAR MANIAMMAI INSTITUTE OF SCIENCE AND TECHNOLOGY
TANJAVUR, INDIA

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
PERIYAR MANIAMMAI INSTITUTE OF SCIENCE AND TECHNOLOGY
TANJAVUR, INDIA