Enhanced Security System of Internet of Things data streaming

Ahmed Saada
Information systems
Faculty of Computer and Information science, Al-manoufia University
Shebin El-Kom, Egypt
ahmedsaada989@gmail.com

Hatem Mohamed
Information systems
Faculty of Computer and Information science, Al-manoufia University
Shebin El-Kom, Egypt
hatem.abdelkader@ci.menofia.edu.eg

Asmaa Aly
Information systems
Faculty of Computer and Information science, Al-manoufia University
Shebin El-Kom, Egypt
asmaa.elsayed@ci.menofia.edu.eg

***Abstract*— The Internet of Things (IoT) is projected to be a promising future technology, connecting billions of items via the internet. The demand for making smart devices more secure is growing as the number of smart devices connected to the Internet that deliver various services in many industries grows. At this time of current and future technological growth, the issue of safety is a major concern. Security threats have become a huge threat to our world, posing a threat to everyone who lives on the planet's surface, making it critical to secure internet-connected devices, particularly those with little resources. As a result, in this paper, we will discuss how to secure those devices with limited resources by encrypting data sent through those devices using a proposed lightweight algorithm named Enhanced Secure Internet Of Things (ESIT) that requires a 128-bit key to encrypt a 128-bit block. The ESIT algorithm is considered an optimizer from the SIT Algorithm that requires a 128-bit key to encrypt a 128-bit block. To implement the encryption process in the shortest possible time.**

Keywords— IoT; Security; Encryption

I. INTRODUCTION

There are billions of devices connected to the Internet, and a massive quantity of data is generated by these devices. Protecting the privacy, authentication, and service support of this data in the Internet of Things is a difficult task. In terms of smart transportation, health-care, smart cities, smart homes, virtual power stations, smart grids, and smart devices, the Internet of Things' future is largely tied to public use.

So far, there have been almost 10 billion connected and interacting things on the Internet; presently, there are over 50 billion objects connected to the Internet, and the number of devices connected to the Internet is predicted to reach 1 trillion by the year 2025. [1] The Internet becomes a network of various disparate entities that interact with one another and with humans on the one hand. It is a topic of worry that must be kept in mind in order to ensure that the issues of data confidentiality, integrity, and authenticity that would develop as a result of privacy and security are addressed. [2]

Now, the Internet of Things technology can be used in a variety of fields, including health care, industrial fields, petroleum exploration, transportation and communications regulation, and meteorological forecasting. One of the most important applications that we will address and study ways to maintain the privacy and security of the information transmitted through it is smart devices. To encourage the adaption process, the Internet of Things must guarantee proper protection for its data [3]. IoT use is still in its early stages, although it is growing rapidly [18], [19]. in this paper, we provide an overview of the Internet of Things in a building automation system [20].

[21] claims that several businesses are becoming more interested in embracing IoT. [22], [23] examine the different applications of the Internet of Things in the healthcare industry, and the prospects for improvement in healthcare given by the Internet of Things will be vast. [24].

The Internet of Things is essentially vulnerable to a variety of security risks, and if the necessary security measures are not taken into account, there is a risk of information leakage or economic harm [3], [4]. Such risks are one of the most significant roadblocks in the Internet of Things [5], [6]. Because it is uncensored for such a long time, IoT is vulnerable to attacks [7], [8]. There is a good risk of a physical attack on its components.

"Things" can be connected to the Internet using one of the modern technologies for connecting to networks, such as Bluetooth, ZigBee, WIFI, or others, and what these technologies have resulted in. The Internet of Things is based on a significant shift in the way wireless sensor networks (WSNs) are built. Objects can interact with one other and with humans, allowing for a wide range of new medical, industrial, economic, educational, sporting, and other uses. At the level of the individual's daily life. The issue's foundation is based on a scenario of things interacting through the Internet to deliver the best services to people. However, the security of these services offered to humans has deteriorated. Because the Internet connection of the gadgets that provide these services has become unsecure. We will go through basic and technical strategies for securing smart devices with little resources.

Basic methods

As previously said, Wi-Fi technology allows things or devices to connect to the Internet. As a result, IoT networks and devices must be secured by locking the front entrance and securing the router. A hacker who gains access of your router also has control of your network, which means they can manage any device in your home, from door locks to computers. Change the router's name and password. Don't rely on the default options. Routers are frequently named for the brand or network they're connected to, giving hackers a crucial hint as to which kind of access they're utilizing.

It's also a good idea to avoid using your real name or address, as this can be a clue that someone is attempting to break into

your network. Use strong passwords, which are made up of a combination of the alphabet, letters, and symbols. The well-known F-Secure firm had a different viewpoint, suggesting that a router devoted to smart devices be designed, along with an antivirus to secure these devices from intrusions. Norton has also created a new router called Norton Core that connects various smart gadgets to the Internet. Unfortunately, the router provided by Internet service providers is insufficient to defend the network from intrusion. Visit PC Mag or Small Net Builder to learn about the best routers and how to safeguard your network. Regardless of whatever router you choose, there are a few things to consider to ensure that it is very secure: -

The first one:
As previously stated, the default password for accessing this router's settings must be changed. Unfortunately, most breaches are caused by the default password.

Second:
Wi-Fi Protected Setup (WPS) This feature must be turned off. Because this functionality allows devices to join through pin code rather than a Wi-Fi password, and this pin code can be hacked in within ten minutes.

Third:
Disable the Universal Plug and Play (upnp) feature, which simplifies the process of transferring ports or ports for connection to the router from some network devices or programmes.

Fourth:
the tr069 or cwmp functionality, This is a protocol used by your Internet service provider to control your router via its own server in order to make essential router updates[9]. Unfortunately, this vulnerability is one of the most commonly exploited by router hackers, and it is one of the causes of the TE Data Wi-Fi router hacking tragedy. Millions of routers are vulnerable to hacking in the aforementioned methods, according to Lucian Constantin and other information security specialists. [9]
This is a setting for the router. In terms of your Wi-Fi network, you should set a strong password, enable network encryption through the router's settings, select WPA encryption and the AES Algorithm, and change the network's default name, because most hackers will know the router's type and thus exploit its flaws to gain access to your network. One of the most significant applications and tools for defending against cyber attacks and incursions is a firewall. To prevent hacker attacks, this tool must be enabled in the router's settings. After you've completed all of these tasks, you'll need to test the security router's strength using various worldwide and well-known websites, such as shields up [10]or the router check program on your mobile phone. The router, once again, is the point at which electrical devices are connected to the Internet. These gadgets will be vulnerable if they are not adequately secured.

Technical methods.

IoT components are inefficient in terms of both energy consumption and processing power. The performance of power-constrained devices will be hampered by the computationally expensive implementation of existing security techniques.
According to an HP study, 70 percent of Internet of Things devices are vulnerable to assaults [11]. The assault is known as a man in the middle attack because it is carried out by sensing the link between two nodes. To counter such attacks, no credible method has been provided. Encryption, on the other hand, may limit the amount of data integrity harm. A safety system is required to assure data homogeneity when storing in the middle warehouse and also during transportation.
Various encryption techniques that handle the abovementioned command have been created, but their application in IoT is debatable because the devices we interact with in the Internet of Things aren't designed to implement computationally expensive encryption algorithms. To achieve the security needs at a low accounting cost, a trade-off should be made.

II. RELATED WORK

Many IoT devices are classified as low-resource devices due to limited resources. Area, memory size, computing power, power usage, and energy are examples of such resources. We need a lightweight encryption system that fits with these constrained resources because traditional security approaches demand more compute power and resources. Lightweight cyphers have gone through three stages in order to show how research progresses.

Noekeon, Iceberg, Des, Tea [15], Camelia, and Idea are examples of this stage, which spanned the 1980s and 1990s. Present[16], mCrypton, Present[16], Puffin-2, Klein, Led, PPRINTcipher, Sea, Clefia, Desl/Desxl, MIBS, and TWIS are examples of the second phase, which spans around 2005-2012. The focus of optimization has recently changed from space reduction to security and latency improvements.
Picaro, Simon [17], Zorro, Prince, Rectangle, I-Present, Pride, ITUbee, FeW, Robin and Fantomas, Hisec, Speck, Lea, Halka, and Present-GRP are some recent examples. However, the downsides of these algorithms are that they require several rounds of encryption and hence take longer to complete, which is a major issue for devices with limited resources.
Consequently, So, to tackle the concerns of rounds and time, Researsher uses a new algorithm called SIT (13) They use entropy and correlation to test the security strength of the sat algorithm.
Correlation is a term used to describe the relationship between two values. It's a statistical relationship that shows how one value is dependent on another. The correlation value of data points with a high reliance is high. The ciphertext reliance in the original message should be removed by good encoding [13]. As a result, no information can be recovered only from the coding, and no relationship between the ciphertext and the plain text can be established [13]. Shannon's theory of communication of secrecy systems described this requirement.
We calculated the correlation coefficient of the original and encrypted photos in this experiment. Original and encrypted

image correlation coefficients. Equation is used to calculate the correlation coefficient (2). Should be equal to 0 in the optimal coding case and 1 in the worst case scenario.

$$\Upsilon_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)\sqrt{D(y)}}}, \quad (2)$$

The variances and covariances of the variables y and x are represented by (y), (x), and cov(x,y), respectively. The equation can be used to calculate the spread of values or variance of any single dimension random variable (3).

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (3)$$

With (x) represents the variance variable x.
The covariance between two random variables x and y, $c(x,y)$ s expressed as follow:

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (4)$$

In equations 3 and 4, the quantities (y) and (x) represents respectively the expected values of the random variables y and x. These expectations are computed by using the following formula:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (16)$$

With N is the total number of pixels in the image and is equal to $row \times col$, x is a vector having N as length and xi represents the ith intensity values of the original image.
Image Entropy: The encryption technique adds additional information to the data, making it harder for the intruder to distinguish between the original data and the algorithm's additions. The amount of information is assessed in terms of entropy, and the higher the entropy, the better the security algorithm's performance. Equation (1) is applied to the intensity (I) values to get the entropy (H) for a picture, where (Ii) is the intensity value probability Ii.

$$H(I) = -\sum_{i=1}^{2^8} P(I_i) log_b(P(I_i)) \quad (1)$$

The disparity between the original data and the encoded data is demonstrated by the correlation comparison in table.1. The original data, in this case an image, can be regarded strongly correlated and has a high correlation coefficient value. The encrypted image, on the other hand, does not appear to have any link that provides strength.
The sat algorithm was used to encrypt a number of photos (Lena, Baboon, Cameraman, and Panda), each image taking an average of 18.42 seconds to encrypt, and the correlation and entropy coefficient were calculated independently for each image, as shown in Table 1.

Image	Size	Correlation		Entropy	
		Original	Encrypted	Original	Encrypted
Lena	256 x 256	0.9744	0.0012	7.4504	7.9973
Baboon	256 x 256	0.8198	0.0023	7.2316	7.9972
Cameraman	256 x 256	0.9565	0.0012	7.0097	7.9973
Panda	256 x 256	0.9811	0.0022	7.4938	7.9971

TABLE 1: Results for Correlation and Entropy of sit algorithm [13]

The image took an average of 18.42 seconds to encrypt. We upgraded the SIT method by suggesting the ESIT algorithm because the time consumed in the encryption process is high.

III. Proposed Enhansed Secure Internet of Things : ESIT

We will discuss Secure IoT, a lightweight encryption technique for the Internet of Things (ESIT). The proposed algorithm for the Internet of Things is intended to address the previously mentioned security concerns as well as resource constraints. It is thought to be an improvement in the performance of the sat algorithm [13] to speed up the encryption process. The need for lightweight cryptography has been widely explored [12], [14], as well as the Internet of Things' limits in terms of constrained devices. Some lightweight encryption algorithms, in reality, don't always take advantage of security efficiency trade-offs. Between the functionalities of block cypher, stream cypher, and hash, block cypher performed significantly better.
ESIT is a symmetric key block cypher with a key of 128 bits and plain text of 128 bits. It will be used to encrypt a quantized voice image, which is one of the data images sent and received by smart devices with restricted resources. Figure 1 shows a diagram of a potential encryption/decryption procedure used to the Internet of Things' quantitative voice picture.

In order to obtain the encoded image, a suggested lightweight encryption technique is applied to the quantitative voice image, as illustrated in Fig. 1. The decoded image is then obtained by using the ESIT algorithm to the encoded image. The quantitative speech signal is then reconstructed, and then de-quantization is applied to the signal to produce the speech output signal that represents the original data.

The following factors are used to evaluate the proposed technology's security:

- The influence of encryption on entropy
- the sensitivity of the key
- the picture and Histogram correlation

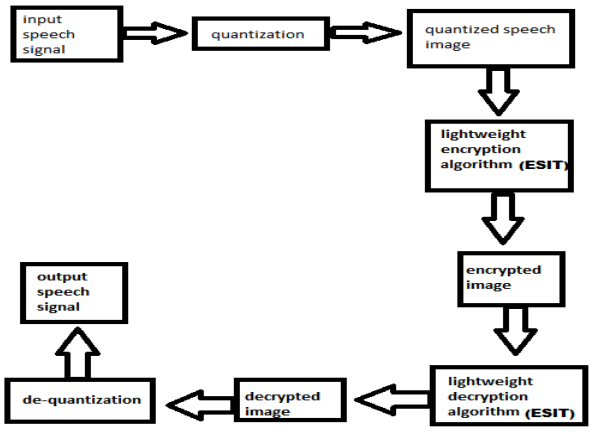

Fig. 1.diagram of a proposed encryption technique applied to the quantized speech image of the Secure IOT .

A. ESIT

In light of the [13] execution time, we will utilize a block cypher with 128-bit plain text and a 128-bit key to reduce the overall time for the encryption execution process while preserving the security rate.

1. The expansion key

Because the suggested algorithm has five rounds of encryption and decryption, we'll need five different keys for this. To do so, we'll use a 128-bit main expansion block. The block will generate five distinct keys after performing considerable operations to cause diffusion and confusion in the input key.

These keys are required for encryption and decryption, and they must be strong enough to stay anonymous throughout an assault. The arrays are turned into four 32-bit arrays called round keys to get round keys, K1, K2, K3, and K4.

This is depicted in the following diagram:

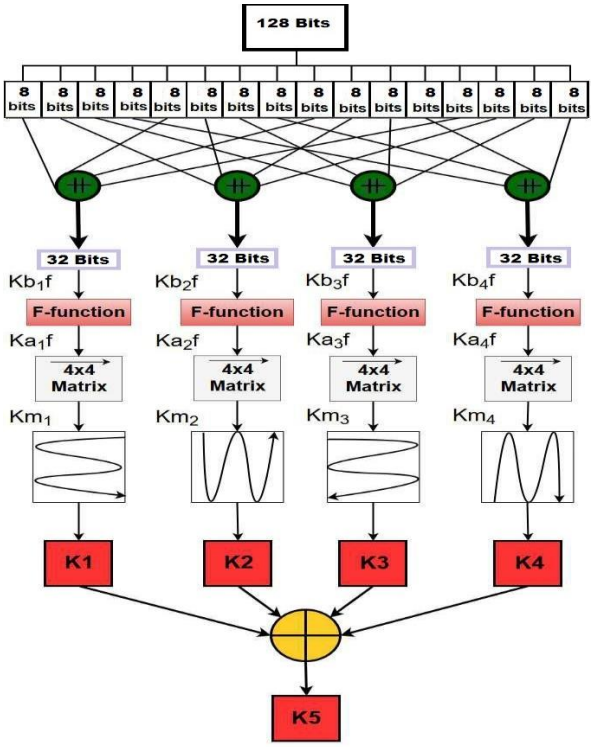

Fig. A: Key Expansion

2. Plain Text and Encryption

The encryption process can begin after the round keys have been produced. This procedure comprises of some logic operations, such as shifting left, swapping, and replacement, for the purpose of causing perversion and confusion. B. Illustration As seen in the coding process, a group of 128-bit plain text is divided into four 32-bit segments.

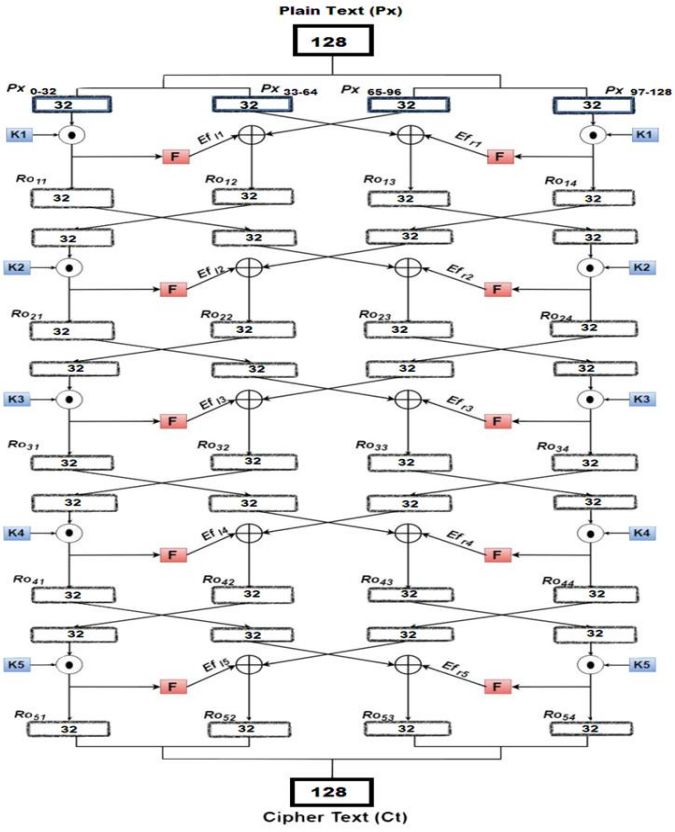

Fig. B: Encryption Process

The bit-plaintext is divided into four 32-bit bits initially. As the bits advance in each round, an interchange is used to lower the data's authenticity by shifting the sequence of the bits, effectively increasing the cypher script's confusion. Between the round keys, a bitwise XNOR operation is done.

IV. Results and Discussion

Using Matlab and a laptop with an Intel Core i3 processor The encryption and decryption processes were performed successfully with the stability of the algorithm's security strength test rates, correlation, and entropy utilizing a block cypher consisting of plain text 128 bits and a key 128 bits. The overall time for the implementation process was reduced to 14.5 seconds, which is exactly what we intended to achieve in order to improve this technique. Figures 2, 3, 4, and 5 show the encryption, correlation test, and histogram findings, respectively.

Size of the Quantized Speech Image	Correlation		Entropy	
	Original Quantized Speech Image	Encrypted Quantized Speech Image	Original Quantized Speech Image	Encrypted Quantized Speech Image
256*256	0.9744	0.0023	7.4509	7.9968
Total encryption time (in Second)				
14.530013				

TABLE 2. Results for Correlation and Entropy after improving the algorithm.

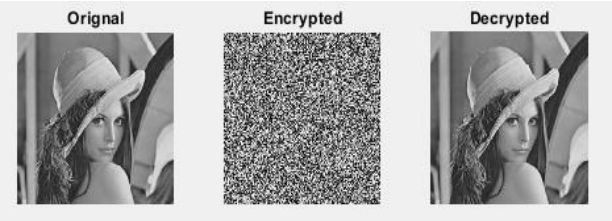

Fig. 2.Image Encrypted / Decrypted

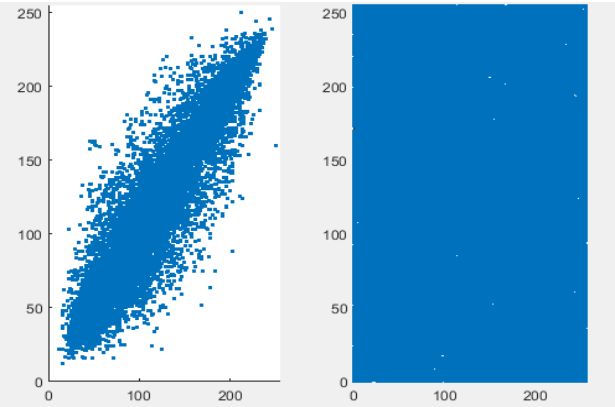

Fig. 3. Correlation comparison.

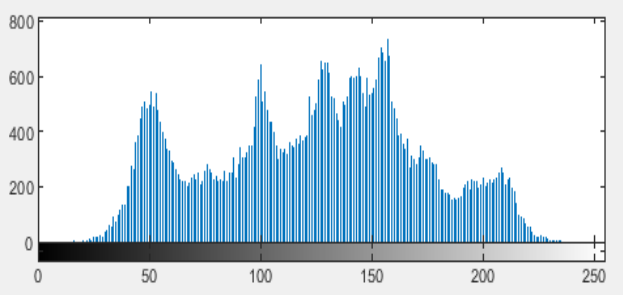

Fig. 4. Histogram:Lena original

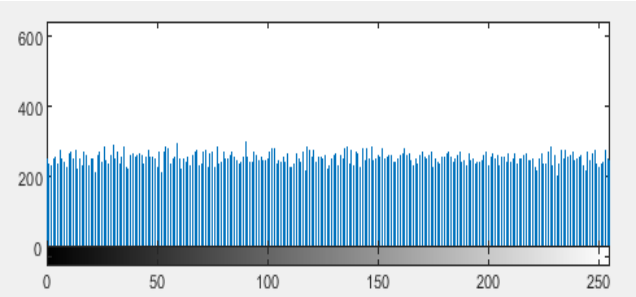

Fig. 5. Histogram:Lena encrypted

Another way to speed up the encryption process is to lower the image size to 128 pixels rather than 256 pixels, which would result in a total execution time of 4.0780 seconds while keeping the same level of security. Figures 6, 7, 8 and 9 show the results.

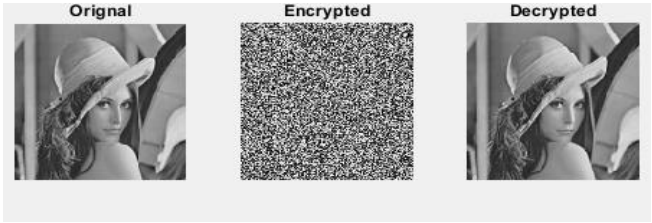

Fig. 6. Image Encrypted / Decrypted

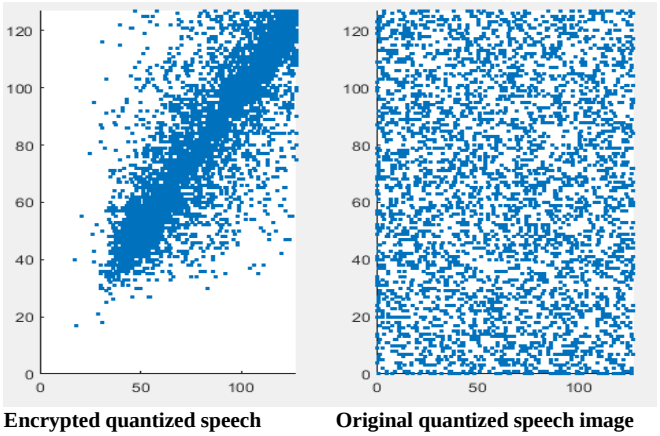

Fig. 7. Correlation comparison.

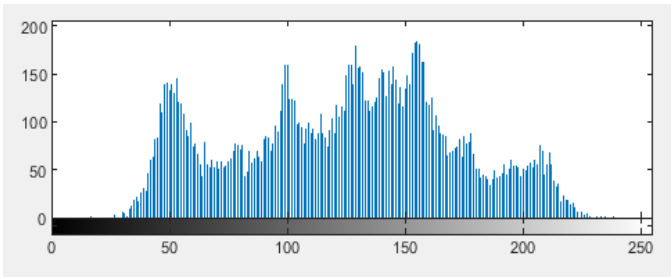

Fig. 8. Histogram:Lena original

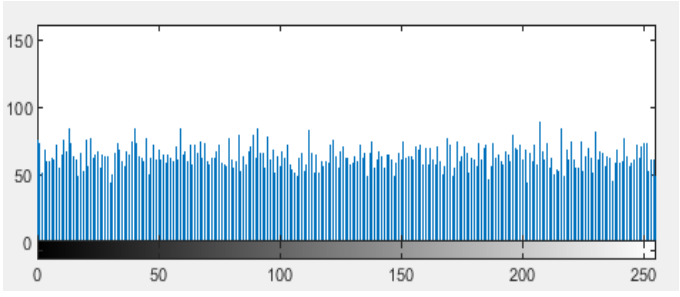

Fig. 9. Histogram:Lena encrypted

V. FUTURE WORK

The Esit algorithm has been implemented in one type of data transferred through smart devices in the iot environment, which is images, but in the near future, I recommend implementing this lightweight algorithm on all types of data, such as audio and video files and others, in order to ensure sufficient security for these devices in light of the limited resources available to her.

CONCLUSION

The Internet of Things (IoT) is a critical component of our daily lives. The number of devices connected to the Internet rises every day, yet these devices are still constrained in terms of energy and resources, and they must be maintained by security systems despite this. While preserving data transfer speed through it. To improve the execution time of the encryption process for data transmitted through these devices with limited resources, the ESIT algorithm has been proposed, which is done by improving SIT algorithm, and its implementation has shown promising results, making the algorithm a suitable candidate for adoption in IoT applications.

REFERENCES

1) D. Airehrour, J. Gutierrez, and S. K. Ray, ―Secure routing for internet of things: A survey, ‖ Journal of Network and Computer Applications, vol. 66, pp. 198 – 213, 2016.

2) H. Suo, J. Wan, C. Zou, and J. Liu, ―Security in the internet of things: a review, ‖ in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648 – 651.

3) J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

4) H. J. Ban, J. Choi, and N. Kang, "Fine-grained support of security services for resource constrained internet of things," International Journal of Distributed Sensor Networks, vol. 2016, 2016.

5) S. Khan, M. Ebrahim, and K. A. Khan, "Performance evaluation of secure force symmetric key algorithm," 2015.

6) P. L. L. P. Pan Wang, Professor Sohail Chaudhry, S. Li, T. Tryfonas, and H. Li, "The internet of things: a security point of view," Internet Research, vol. 26, no. 2, pp. 337–359, 2016.

7) M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata, "Lightweight and escrow-less authenticated key agreement for the internet of things," Computer Communications, 2016.

8) L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.

9) lucian-Constantin, https://www.csoonline.com /Lucian-Constantin, 2014

10) Steve Gibson , Port Authority Edition – Internet Vulnerability Profiling by Steve Gibson, Gibson Research Corporation https://www.grc.com/x/ne.dll?bh0bkyd2,2020

11) S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," in 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016, pp. 5772–5781.

12) M. Katagi and S. Moriai, "Lightweight cryptography for the internet of things," Sony Corporation, pp. 7–10, 2008.

13) Muhammad Usman, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan and Usman Ali Shahy, ''SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,'' International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.

14) M. Ebrahim, S. Khan, and S. S. U. H. Mohani, "Peer-to-peer network simulators: an analytical review," arXiv preprint arXiv:1405.0400, 2014.

15) Kataoka, H., Sawada, A., Duolikun, D., Enokido, T.: Energy-aware server selection algorithms in a scalable cluster. In: International Conference on Advanced Information Networking and Applications. IEEE (2016)

16) Rolfes,C., Poschmann, A., Leander, G., Paar,C.: Ultra-Lightweight Implementations for Smart Devices—Security for 1000 Gate Equivalents. Springer, Germany (2008)

17) Beaulieu, R., Shors, D., Smith, J., Treatment-Clark, S., Weeks, B., Wingers, L.: Simon and Speck: Block Ciphers for the Internet of Things. NIST Lightweight Cryptography (2015)

18) D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.

19) L. Da Xu, "Enterprise systems: state-of-the-art and future trends," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 630–640, 2011.

20) P. Zhao, T. Peffer, R. Narayanamurthy, G. Fierro, P. Raftery, S. Kaam, and J. Kim, "Getting into the zone: how the internet of things can improve energy efficiency and demand response in a commercial building," 2016.

21) Y. Li, M. Hou, H. Liu, and Y. Liu, “Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of internet of things,” Information Technology and Management, vol. 13, no. 4, pp. 205–216, 2012.

22) Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, “Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things,” in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, pp. 529–534.

23) S. Misra, M. Maheswaran, and S. Hashmi, “Security challenges and approaches in internet of things,” 2016.

24) M. C. Domingo, “An overview of the internet of things for people with disabilities,” Journal of Network and Computer Applications, vol. 35, no. 2, pp. 584–596, 2012.