Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Performance Enhancement of Security Mechanism of IoT-5G Systems

[1]Pratik Shah, [2]Dr. Deepika Pathak

[1]Research Scholar, Dr. APJ Abdul Kalam University, Indore
[2]Professor**,** Dr. APJ Abdul Kalam University, Indore

1. Introduction

The need for Internet of Things (IoT) devices is growing daily, and many businesses are creating various kinds of IoT-enabled gadgets. IoT devices employ sensors to gather information from the environment and nearby areas. They then process the information and use the information to take further action. IoT devices are widely used in many different fields, such as agriculture, where they are used to monitor soil moisture, smart cities, hospitals, and manufacturing companies. They are also used to manage parking, detect leaks, measure water levels, and automatically turn on or off machinery based on predetermined conditions [1]. IoT devices offer automation that requires less human intervention.

Things and the Internet combine to make IoT. The Internet is a collection of networks inside networks that offers a variety of sharing options, including data and resources. Things include things like air conditioners, microwaves, street lights, autos, and so on that are smart objects. In essence, IoT enables these gadgets to be connected to the Internet and operates with fewer human interaction [2]. The goal of the Internet of Things is to increase machine-to-machine contact while reducing human-machine interaction. The Internet of Things is made up of a number of parts, including networking systems, sensors, actuators, protocols, and cloud services. The IoT architecture is primarily composed of four levels, each of which has specific characteristics shown below [3]:

- Sensing Layer: Data collection is the responsibility of this layer. The sensor and actuator, which make up this layer, are in charge of gathering environmental data such as light, temperature, humidity, and moisture content.
- Network Layer: This layer facilitates data sharing with the cloud for data analysis and storage, as well as communication between Internet of Things devices. Mobile networks, Bluetooth, and Wi-Fi are a few examples of the network layer. To securely transfer data, this layer also carries out encryption and decryption.
- Data Processing Layer: at order to summarize the information, raw data is received and processed further at this layer. This layer includes many data analysis techniques as well as the database management system.
- Application Layer: The Application layer is the top layer in an IoT architecture. This layer offers an interactive environment where users may obtain processed data created by the Data Processing Layer or direct IoT devices using any application program or website.

2. Literature Review

Sensors, actuators, and other electronic components make up Internet of Things (IoT) devices. These components operate under a number of constraints, including a low power supply, a restricted processing capacity, a small amount of memory for storing data, and a constant Internet connection [4]. Because of this poor data security, the majority of IoT devices are unable to protect against any attacks.

Following are the limitations of IoT which needs to be improved for improving the performance of these devices [5]:

- Lower CPU speed: Due to their compact size and restricted power supply, these devices have a lower CPU processing speed than other devices. As a result, they are unable to do longer computations.

- Insufficient Memory for storing: As a result of the device's reduced processing power, manufacturers utilize less memory for storing. Certainly, less memory will also use less electricity.
- Password dependence for data security: It is never advisable to rely just on a strong password for data security; there are undoubtedly a number of additional considerations that must be taken into account.
- Employ of subpar cryptographic solutions: It is advised to employ sophisticated machine learning-based cryptographic solutions to safeguard data on Internet of Things devices because they have less memory and processing power. However, the majority of these devices use subpar cryptographic solutions.
- Updates are not required: Users do not update the software on IoT devices, and manufacturers do not offer remedies to the most recent danger since the device is not aware of it.

There are four layers in an IoT device, and researchers have looked into four different attack vectors:

- Physical Layer assault: This type of assault aims to interfere with sensors' and actuators' ability to function.
- Network Layer Attack: This layer of attack causes harm to the communication route that Internet of Things devices utilize to connect with one another.
- Encryption Layer assault: This assault targets the encryption system employed by Internet of Things devices, rendering data privacy obsolete.
- Software Layer Attack: This type of attack introduces errors into the IoT device's system software.

A technique for producing worm attack predictions has been suggested by [6]. Using this technique, network traffic data is analyzed in real time to forecast potential worm attacks. The time series formula and linear regression are used to determine the attack prediction. The findings indicate that the success rate of worm prediction is higher than that of the prior techniques; the method's main drawback is that it is only effective for worm detection and not for other kinds of attacks.

In order to comprehend how attack strategies evolve over time, [7] have examined a number of attack projection frameworks. Based on their research, they developed a model that forecasts the upcoming assault based on the many kinds of attacks that have been identified in the past. Through the use of the footprints that are extracted from multistage assaults, this attack projection study allowed them to develop a plan for identifying the next attack [8]. In this way, the next assault is anticipated, although it is undoubtedly difficult to extract footprints for such a large network.

[9] have researched a number of forecasting techniques for power supply outages in smart grids. ANNs, or artificial neural networks, are being used to make predictions based on data gathered from various smart grid locations. This data is being utilized to produce a map that will aid in making forecasts about impending power outages. With the use of ANN, they teach the computer to comprehend the map. The computer was not easily trained, though, because a lot of data was gathered from the smart grid, the procedure was intricate, and the system's output was limited to certain circumstances [10].

3. Proposed Work

In order to maintain security and privacy of data during communication between IoT devices, cryptography plays a vital role. In this paper a data security methodology were proposed, implemented and comparative study done, to evaluate the performance of the proposed one. The proposed methodology is, Boltzmann Machine is used to generate keys, to encrypt message and decrypt message.

The keys are generated dynamically, robustly, and efficiently via the encryption and decryption process using a Restricted Boltzmann Machine Algorithm based on Deep Learning. The following justifies the usage of restricted Boltzmann machines:

- Mutual authentication: this describes the procedure that has to be followed for authentication when two devices are going to share data.
- Privacy: Privacy refers to the idea that identity disclosures should not occur during data exchanges between Internet of Things devices.

- Exchange of Session Keys: When exchanging session keys, preserving their security should come first.
- Defense Against assault: this refers to putting defenses in place during an assault with the intention of protecting devices and data.

RBM - Restricted Boltzmann Machine distribution is used to generate secured cryptographic key by using the modified formula as follows:

$$P_i = \frac{e^{\left(-\varepsilon_i/kT\right)}}{\sum e^{\left(-\varepsilon_j/kT\right)}} - \left(\sum_{i<j} w_{ij}\, s_i\, s_j + \sum_i \theta_i\, s_i\right) \quad \text{..... (1)}$$

$$P_i = \frac{\varnothing e^{\left(-\varepsilon_i/kT\right)}}{\sum e^{\left(-\varepsilon_j/kT\right)}} - \left(\sum_{i<j} w_{ij}\, s_i\, s_j\right) \quad \text{..... (2)}$$

In the suggested formula above the symbols Pi stand for probability of a system in its initial state, T for system temperature, k for Boltzmann constant, and He(-ϵ/kT) for all possible system states. Equation (1) will be utilized for message encryption, while equation (2) will be utilized for message decryption.

Within RBM, nodes may be classified as either visible or hidden, and both display unique characteristics. A hidden node cannot interact with another hidden node, and a visible node cannot communicate with another visible node. However, hidden and visible nodes can communicate with one another. The suggested technique uses a dataset that is downloaded from Kaggle for training.

Contrastive Divergence: The primary function of RBM is to modify the nodes' weights. To achieve this, RBM employs weighing techniques that are comparable to assigning some fresh, random beginning weights. Gibbs sampling is the method used to alter the weights. The well-connected and multilayer node model is effectively trained using the suggested methods.

The suggested method, which makes use of a restricted Boltzmann machine, is shown to be more dynamic and a fully functioning asymmetric key generator. The encryption and decryption processes are carried out by combining RBM with the suggested formula. It is discovered that the procedure modifies every character when the approach is checked to see how it functions. Data encryption is accomplished by masking the set's eight-bit input in a single layer of eight neurons. It is discovered that the encrypted text is included in the eight-dimensional vector, which is an array of floating-point values of eight length when multiplied by the supplied data. The output layer, which comprises twelve-dimensional floating-point vectors and floating-point values, is used for decryption. The formula to obtain the result is obtained by using the Boltzmann Machine Distribution function.

The suggested work's performance was analyzed by taking into account two parameters: encryption and decryption times. Python is used in the implementation of the proposed task. Files containing 600KB, 800KB, 6MB, 12MB, 40 MB, 100MB, and 150MB random datasets were generated. To find the amount of time needed for encryption and decryption, use the timeit() method in the timeit module of Python. The Timeit() method returns the time in seconds; however, because the number is in decimals, it must be converted to milliseconds in order to make it easier to compare with other values and have a larger value.

The results produced by the suggested work is shown in Figure 1, and when the findings are contrasted with those of other well-known cryptosystems, it is discovered that the suggested work completes encryption and decryption faster than the others.

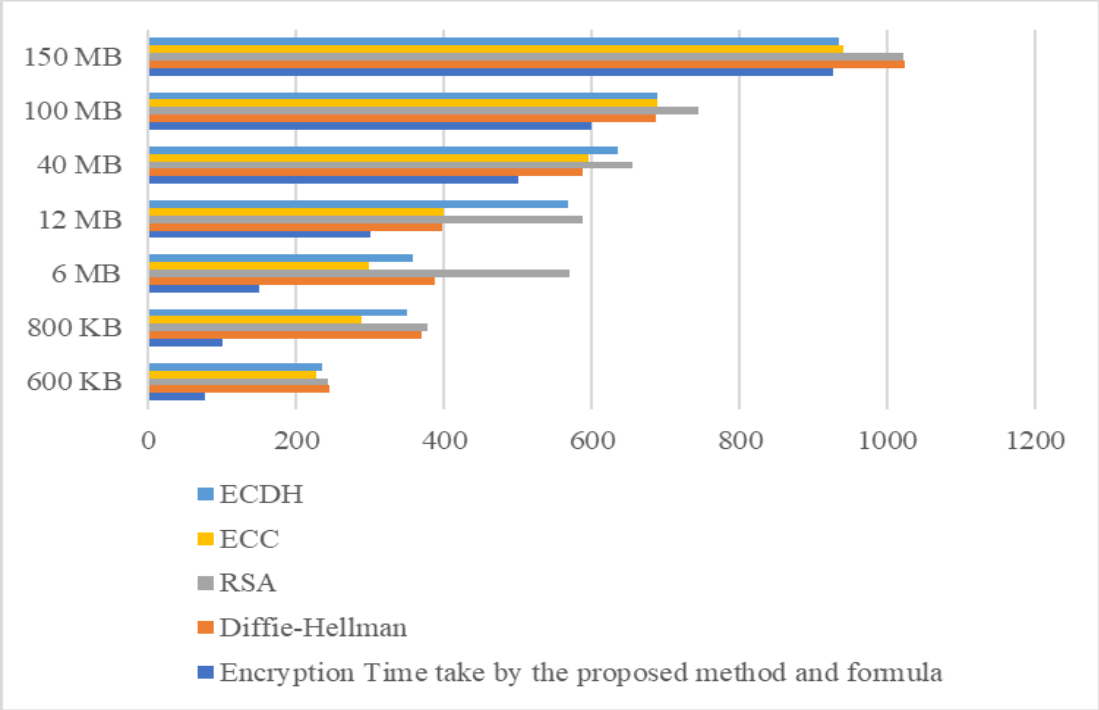

Figure 1: Encryption Time by the proposed work and others

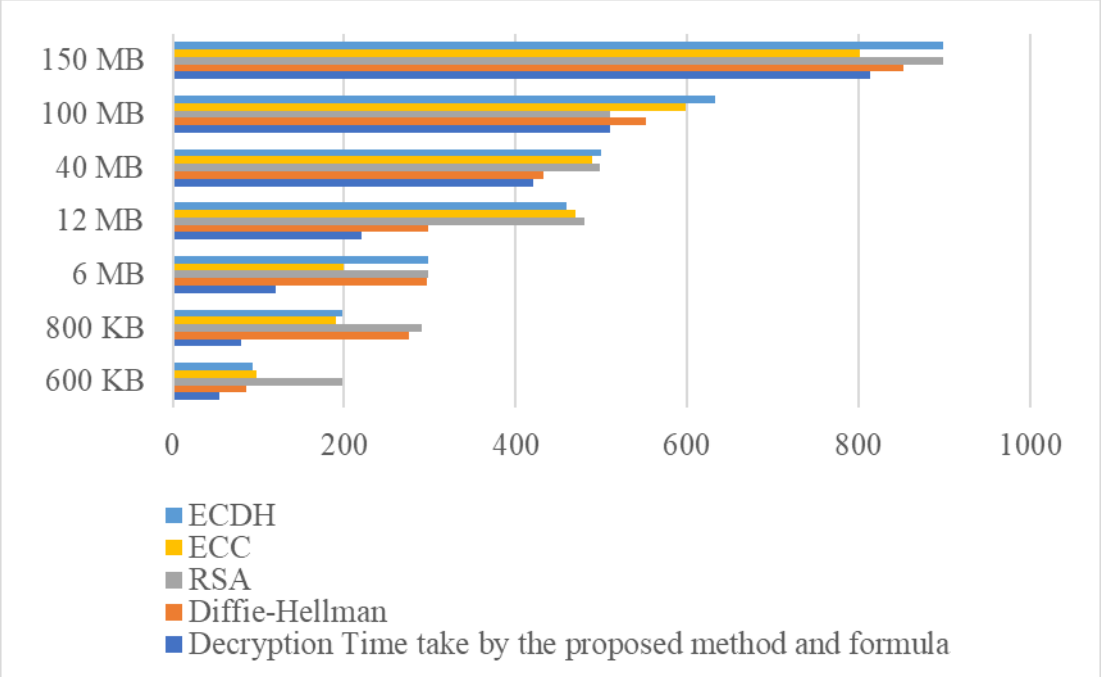

Figure 2: Decryption Time by the proposed work and others

4. Conclusion

Concerns regarding the future of data security of IoT 5G systems are many due to the highly dynamic nature of the technology sector, the increasing speed and lowering latency of networks, and the massive volumes of data generated by IoT devices. Data security will always be a problem. Regular updates of security procedures are necessary to ensure that devices are ready to repel new threats and attacks. It is essential to keep in mind that everyone is responsible for keeping an eye on data security. Manufacturers, developers, and individuals should routinely evaluate their data security protocols with the most recent data security principles to guarantee that data is constantly secure.

References

[1] A. K. Lenstra and B. M. M. Weger, “Twin RSA," Advances in Cryptology, 2021, vol. 15, pp. 222-228.
[2] S. D. Galbraith, C. Heneghan, and J. F. McKee, “Tuneable balancing of RSA," Journal of Information Security and Privacy, 2005, vol. 4, pp. 280-292.
[3] H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, “Dual RSA and its security analysis," IEEE Transactions on Information Theory, 2021, vol. 53, pp. 2922-2933.
[4] S. J. Aboud, M. A. Al-Fayoumi, M. Al-Fayoumi, and H. S. Jabbar, “An efficient RSA public key encryption scheme," International Conference on Information Technology, 2008, pp. 127-130.
[5] M. Bahadori, M. R. Mali, O. Sarbishei, M. Atarodi, and M. Sharifkhani, “A novel approach for secure and fast generation of RSA public and private keys on smartcard," 8th IEEE International NEWCAS Conference, 2010, pp. 265-268.
[6] A. Chhabra and S. Mathur, “Modified RSA algorithm: A secure approach,’’ International Conference on Computing Intelligence and Communication Networks, 2011, pp. 545-548.
[7] S. Sharma, P. Sharma, and R. S. Dhakar, “RSA algorithm using modified subset sum cryptosystem," 3rd International Conference on Communication and Computational Technologies, 2021, pp. 457-461.
[8] A. H. Al-Hamami and I. A. Aldariseh, “Enhanced method for RSA cryptosystem algorithm," International Conference on Advanced Computer Science Applications and Technologies, 2012, pp. 402-408.
[9] B. P. U. Ivy, P. Mandiwa, and M. Kumar, ``A modified RSA cryptosystem based on `n' prime numbers," International Journal of Engineering and Computer Science, 2012, vol. 1, pp. 63-66.
[10] S. A. Nagar and S. Alshamma, “High speed implementation of RSA algorithm with modified keys exchange," International Conference on Sciences of Electronics, Technologies of Information and Telecommunications, 2021, pp. 639-642.