MACHINE LEARNING BASED SECURED DATA TRANSMISSION FOR BANKING APPLICATION

Indrani Palanisamy[1], Dr. T. Santha[2]

[1]Research Scholar, Department of Computer Science, Dr. GRD College of Science, Bharathiar University, Coimbatore, Tamilnadu
[2]Principal, Dr. GRD College of Science, Bharathiar University, Coimbatore, Tamilnadu
[1]indraniarul@gmail.com, [2]sandhevya99@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: Security in the Internet of Things emphasizes on securing the Internet-enabled gadgets that link to wireless networks. IoT Safety attempts to safeguard IoT devices and systems against cybercrime and it is considered to be a vital security element linked to the Internet of Things. Conversely, banking applications are progressively being supervised for their failure to provide a sufficient degree of customer support and to protect themselves against and respond to cyber-attacks. One of the main factors for this is the vulnerability of fintech systems and networks to malfunctioning. Therefore, wireless networks covering these IoT products are extremely unprotected. IoT is a lightweight system and it is optimal when using lightweight and energy-efficient cryptography for protection. Deep learning is an efficient technique to analyze threats and respond to attacks and security incidents. So this work addresses both security and energy efficiency in IoT using two novel techniques carried out through deep learning. This work contributes to the most innovative way of saving energy in IoT devices through decreasing the use of energy-expensive '1' values in the interface of Dynamic RAM. This can be done by using Base + XOR encoding of data during data transmission. Also, the security of data is incorporated using chaotic XOR encryption (CXE) algorithm which is proved to perform faster and stronger encryption using XOR operation. Using Conditional Generative Adversarial Network (CGAN) based deep learning technique, the Base + XOR encoding technique and CXE are trained well in the banking application. The data generation in CGAN is carried out based on criteria produced using generator model. This work is proved to be consuming less energy, less data transmission time, and provides more security when compared to the existing systems.

Keywords: Base + XOR, CXE, CGAN, data transmission, IoT devices, Security

1. Introduction

The Internet of Things (IoT) ecosystem has redefined the term "connectivity", with novel paradigms such as smart homes, smart cities, etc., and leading to hitherto unseen human-machine interactions. However, IoT vendors seem to assign higher priority to rapid prototyping and deployment which often leads to the production of devices with multiple security vulnerabilities. [Ramalingam and Venkatesan 19] characterized banking as one of the significant domains that can utilise IoT technology's bright prospects. At present, Automated Teller Machine (ATM), mobile banking and the Point of Service (POS) terminal has become the edge of the banking infrastructure. Banking IoT faces a number of challenges, like data density and privacy, security as well as the necessity to protect customer data. This work solves the problem of data security through conditional GAN. The Generative Adversarial Network (GAN) seems to be a deep learning, uncontrolled machine learning method. In this method, new data along with same statistics that acts as a training set was produced through learning if the training set was given. Generator-The Discriminator Model is a multilayer perceptron (MLP). The purpose of the generator is to model or produce data which is very close to training data. For distribution learning, GAN becomes a new category of generative methods. Like the target distribution, pdata, samples are generated in GAN and it has an aim to learn about a model. In this work, the GAN is introduced to the data transmission process along with protection and also it detects an attack during transmission, Here, in between the generator, G, and the discriminator, D, min-max two player's game is presented. The discriminator D gains knowledge about the differences between the produced data by actual data set and generated data by generator. The generator G also gains knowledge about creating errors while making samples in discriminatory networks. By exposing few additional data (m) to the generator (G) and the discriminator (D), [Jason 19] conducted a presentation on conditional model. In this work, the conditional GAN design transforms the conditioning information, m, into the generator (G) as well as the discriminator (D) as an additional input. This work used two types of conditioning information which are added in both generator and discriminator. BASE + XOR is one of the encoding mechanism. It is performed in the generator of proposed work and it consumes less energy during data transmission.

By executing a basic XOR value operation inside a transaction, the encoding of similar data elements are done through the Base +XOR encoding. CXE is another type of encoding mechanism which encodes the data from BASE + XOR encoded result. It performs stronger and faster encryption using XOR operation. The contribution of this work is as follows.

- Banking data are collected from POS i.e. transmitter and this data is transferred to the generator. The generator performs encoding (BASE + XOR) on transferred data and then it is encoded again using the CXE technique.
- The final encoded result, as well as real data, is transferred to the discriminator which performs the decoding mechanism and it is used to differentiate the encoded data and real data. Then, the real data is sent to the banking service i.e. receiver. The encoded data is sent to the unauthorized person when attacked.

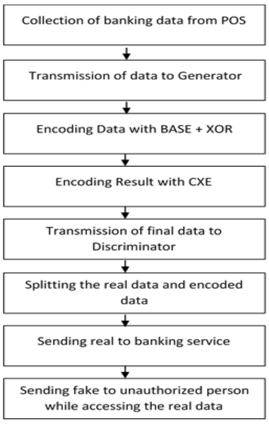
Collection of banking data from POS
Transmission of data to Generator
Encoding Data with BASE + XOR
Encoding Result with CXE
Transmission of final data to Discriminator
Splitting the real data and encoded data
Sending real to banking service
Sending fake to unauthorized person while accessing the real data

Figure 1: Flow diagram

The organization of the work includes the following sections. Section 1 covers the introduction, section 2 covers a literature survey that is used as a guideline of this work implementation. Section 3 provides the proposed work. It has an encoding mechanism and deep learning-based data transmission, section 4 covers the results and discussion and the evaluation of proposed techniques. Lasly, the conclusion part is presented in section 5.

2. Literature Survey

[Farooq et al., 19] proposed the two Generative Adversarial Network (GAN) based models to detect threats in IoT devices from within and outside the network. They also analyzed a use case for network function virtualization for device management once a malicious device has been detected on the network. Their GAN based model mapped the latent space of appropriate dataset of IoT devices and flagged malicious devices found deviating from their norm.

[Hao et al., 18] presented a wireless end-to-end communication method with the help of Deep Neural Networks (DNNs). Following this, Conditional Generative Adversarial Network (GAN) was applied to represent channel effects. The conditioning information was acted by transmitter’s signal which is encoded. For handling time varying signal, the received signal was attached to the pilot data and it was a part of conditioning information.

Secure Wireless Sensor Network Middleware (SWSNM) was discussed by [Remah et al., 18] and it is dependent on the generative adversarial network algorithm which is a unsupervised learning method. This proposed network contains two parts: generator (G) and a discriminator (D). To complicate attackers and to safeguard data, the data was made fake similar to original data. These two data can be distinguished using D which have many layers.

[Zhaoqing et al., 19] discussed about latest development of GAns. First, the analysis of basic theory of GANs and variations among various generative models was carried out. Following this, the classification was carried out in derived models of GANs. The training tricks and evaluation metrics was provided and performance was improved through detailed description about GANs application.

[Xiaopu et al., 19] suggested an effective seismic data acquisition technique. This method contains a Compressed Sensing Architecture in Generative Adversarial Network (CSA-GAN). This method was proposed to overcome huge scale seismic data collection problem. To decrease traffic as well as to balance the data transmission, compressed sensing theory was used which is based on data collection architecture.

[Decheng et al., 20] named a novel approach of curve reconstruction through a conditional generative adversarial network (GAN), CR-CGAN and it was introduced to completely synthesize transmission line Galloping curves.. By applying extra constraints to accomplish the complete reconstruction of the galloping curves, they used the modeling capabilities of the newly added GAN as well as introduced a new configuration in the generator-discriminator pair for obtaining good outcomes and also a new refined loss function to enhance the data.

[Zahangir et al., 19] studied the development of the Convolution Neural Network (CNN), Deep Neural Network (DNN), Recurrent Neural Network (RNN), comprising Long Short-Term Memory (LSTM) and Auto-Encoder (AE), Deep Belief Network (DBN), Generative Adversarial Network (GAN), Gated Recurrent Units (GRU), and Deep Reinforcement Learning (DRL) in the field of Deep Learning (DL). Consequently, great advancement have been addressed, like latest variant DL methods which rely on the DL method.

[Akshay et al., 17] suggested a network design motivated through deep residual networks which allow a more expressive pairwise similarity target to be computed efficiently. They also stated that regularization is the secret to learning with small amounts of information and suggested an extra generator approach that relies on the Generative Adversarial Networks, whereby their residual pair-wise network seems to be the discriminator.

[Elhoseny & Hassanien 19] presented a new method in WSN named secure data processing and transmission scheme. The most popular safe clustering based routing algorithms which have been created for WSNs were studied and extensively addressed. The instructions and steps to create a proper solution for protecting the complex cluster network were n clarified while using less energy probably and adjusting to have less computing power. In addition, it intended to construct a WSN stable clustering approach.

[Mohammed et al., 17] suggested a new deep learning-centred data minimization algorithm which 1) reduces data sets while transmission through carrier channels; 2) prevents man-in-the-middle (MITM) data as well as other attacks through modifying the binary representation over the same dataset multiple times: assigning various code words to the same character in various portions of the dataset.

[Bhavnesh et al., 19] stated the effectiveness of error control codes as well as different modulation frameworks for WSN. The study shows that a right option of modulation system as well as error control codes will minimize the energy consumption in the WSN.

While using Forward Error Correction code termed Raptor codes, [Bhanupriya et al., 17] presented an energy-efficient data transmission method in the Binary Erasure Channel situation. Then changes are made in precoder and resulted raptor codes was examined in aspects of energy.

[Donghyuk et al., 18] discussed about data transfer system using minimal energy based on Base and XOR method. Through carrying out XOR operations among data elements inside a one DRAM arrangement, the data-like component was transferred. They tackled two issues affecting the efficacy of their mechanism which includes, i) the frequent presence in transactions containing zero data elements, (ii) the variety within a transaction using the basic scope of data types. Two methods such as Zero Data Remapping as well as Universal Base +XOR Transfer, were defined.

[Ankur et al., 15] developed a new fast and stable chaotic map-based Encryption method for producing a different cipher texts. The proposed cryptanalysis work illustrated the security as well as strength of keys and algorithm. The effectiveness of the encryption scheme was based on the keys count that use the chaotic function produced.

[Bassem et al., 13] presented a new as well as rapid encryption scheme named chaotic encryption algorithm RFCA. The proposed work comprises chaotic cipher which consists of two perturbed maps piecewise linear chaotic map. In specific, this algorithm was sufficient for encrypting data in ZigBee networks whereby it requires robustness and real-time.

3. Methodology

Security in the banking sector is still one of the challenging tasks. Insecurity mostly occurs during data transmission. In this work, the insecurity issues in the banking sector was detected through conditional GAN. The generator performs its process along with real data which is transferred from POS (Point of Service). After completing two sets of encoding processes the generator sends the final encoded data to the discriminator. The discriminator splits the real data and encoded data. Finally, the receiver gets the real data and the interrupter gets the fake data (encoded data) during the attack. To control the POS terminal, edge data transactions are considered to be a connection point in IoT. This makes POS terminals to source the data based on customer aspects. Some of the IoT applications that can adapt the proposed technique are,

- Connected Automotive as banking branches
- Banking on Wearable
- Smart branches
- Blockchain together with IoT

- Home Banking
- Personalisation of programs
- Customer experience
- Leasing finance automation
- Electronic Monitoring Framework for Bank Applications
- Data security risk

The serious problem faced in an IoT apps is the potential risk of data protection. Banks manage their own data collection, POS terminals, and information technology-driven connections to their corresponding branches. There are POS terminals at most retail banks. To capture the various forms of customer data in banking, it conducts edge data interfaces.

The proposed conditional GAN solves the security issues in banking. The conditional GAN is expanded from GAN that works when any additional information is conditioned on the generator and discriminator. The GAN normally conducts following operations, including generator and discriminator. The generator produces fake data equivalent to the actual sample. Discriminators can distinguish between real and fake data. Encoding and decoding processes can be carried out by the conditional GAN. The real data transmitted from the POS is encoded in the generator using the BASE + XOR encoding method. This decreases the energy cost during transmission. The BASE + XOR encoded output can be used for encoding once again by the CXE encoding technique. This is the generator mechanism. Then, the final data encoded by CXE is passed on to the discriminator. The discriminator executes the process of final decoding. The decoding approach seems to be the reverse encoding process and it can be accomplished through the discriminator encoding technique of BASE + XOR and CXE.

After decoding, the discriminator is used to split the real data and fake data or encoded data. It sends the real data to banking service or receiver and fake data to intruder or attacker. Figure 2 shows the architecture of conditioned GAN.

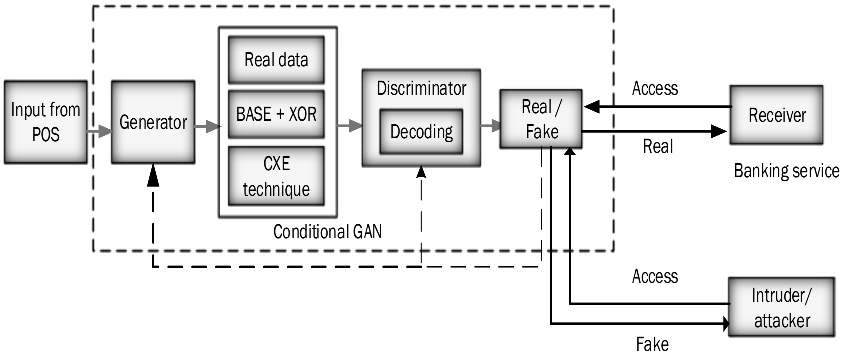

Figure 2: Architecture of conditional GAN

A new encryption method termed chaotic X-OR encryption (CXE) was proposed in this work. This method operates with a base of new chaotic generator and also it is produced from combined two perturbed PWLCM maps.

This works on the basis of new chaotic generator which is generated by the combination of two perturbed PWLCM maps. The proposed method contains the characteristics of a stream cipher generating stochastic noise-shaped pseudorandom bits. This approach focuses on predicting a best stream cipher which can attain both high speed as well as strength simultaneously.

BASE + XOR Operation

Base +XOR is a low energy data transfer method used for encoding a similar portion of data. Inside a transaction, the encoding of XOR operations was performed between data elements. A base element is an unmodified data element. Then encoding is carried out with remaining elements along with the base of the adjacent element as XORed values.

Figure 3 shows the process of proposed work which is used to decrease the energy expenditure of data during transmission. The following steps help to encrypt the banking data i.e. (account number) by BASE + XOR.

- Without making any changes, the element 0 (left-most) which is a 4-byte element are transferred as base element and the base size refers the base element's size.
- Next, the bitwise difference (that is XOR) is performed between the element 1 (which is a second element) and the element 0 (element 0).
- The same process mentioned in above point is carried out between element 1 and element 2 as well as between element 2 and element 3.
- The resulting values are the XORed values and when performing the same XOR operations on XORed elements and their adjacent left elements, the original values of the XORed elements can be attained. All these processes are performed by discriminator.

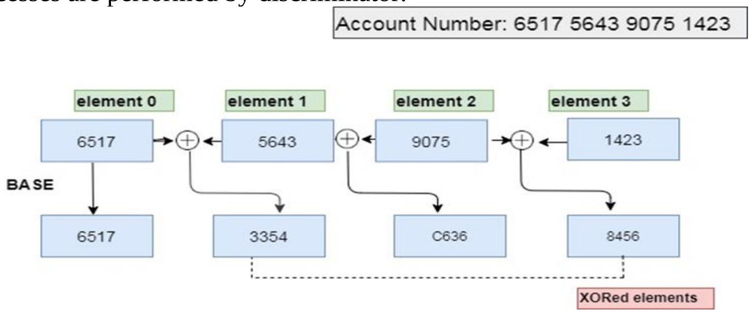

Figure 3: The process of BASE + XOR

1.1 Illustration 1

The first element considered as static and it is a element. Following this, the XOR operation is applied between the static element (element 0) and element 1. The below mentioned XOR elements are described with binary values.

6517- 6=0110 5=0101 1=0001 7=0111,   5643- 5=0101 6=0110 4=0100 3=0011

0 1 1 0 0 1 0 1 0 0 0 1 0 1 1 1 ⊕

<u>0 1 0 1 0 1 1 0 0 1 0 0 0 0 1 1</u>

<u>0 0 1 1</u> <u>0 0 1 1</u> <u>0 1 0 1</u> <u>0 1 0 0</u>

3 3 5 4

1.2 CXE Operation

Chaos functions are usually been used primarily for nonlinear systems to build mathematical models. Due to extreme sensitive nature to starting conditions as well as other fascinating properties, many mathematicians have considered this function. Thus, chaotic systems might provide data encryption and protection with a stable and fast system. The key benefit about utilizing chaos resides in the form of the chaotic signal which appears as noise for illegal users. Furthermore, through simple iterations, chaotic values are mostly created that make chaos appropriate for modeling strong as well as high-speed stream ciphers. To generate the pseudorandom bit stream, chaotic generators use this Chaotic stream ciphers and using the XOR operation the encryption is carried out for already encoded data.

Using BASE + XOR encrypted results, a modern, quick and stable Chaotic XOR-based encryption technique has been proposed. However considering the single or multiple keys for the encryption and decryption process, the encryption and decryption keys are identical at any time. To improve the protection against known cryptanalysis attacks, the different messages were encrypted through various multiple keys. Initially, the number of keys was generated by use of chaos logistic function (logistic map) which provides an initial condition. These keys were forbidden from having any proper conditions, but with these differences and multiple keys, encryption and decryption of all the characters of the information was carried out. Many keys were used to improve both randomness and safety, and a similar key does not need to be encrypted and decrypted with repeated characters in the data. By using the BASE + XOR output, the complexity of keys was improved so that the randomness of keys is improved with improved protection. In secure communication, these complex random keys offered easy, possible as well as efficient encryption, therefore the attacker is not sure regarding key generation. The required notations utilised for the key generation, encryption and decryption process are as follows: R_i = real data; F_i = fake data; E (R_i) = real data encryption; D (F_i) fake data decryption. The below scheme functions (encryption, decryption, and key generation schemes) are conducted as:

For n =1 to j:

$$x_{n+1} = \{A * X_n\ (X_n\ - 1\ )\} MOD\ 256 \qquad (1)$$

In equation 1, A = any integer (1, 2, 3 ...), X_n =Initial value of chaotic function i.e., 2, 3, 4 . . . , j= Number of keys, $x_{n+1} =$ Keys k_1, k_2, k_3, k_4 … $K_{j.}$

1.2.1 Technique for Key Generation

The generation of pseudo-random numbers was proceeded first by utilising the chaotic map function at both ends of the sender as well as receiver.

From equation (1),

Different keys has been produced on conditioning various values of x_{n+1}. And also the number of keys are set through giving few proper criteria like j.

The complex and secure based keys are improved by application of BASE + XOR output of x_{n+1}. Hence, the keys turns to be random as well as don't have any dependency with other keys.

x_{n+1} has been shifted to binary form which is 8-bit

1.2.2 The Process of Encryption

Every Base + XOR output element is expressed in the UNICODE character format that converts its decimal numbers to 8-bit binary numbers. Through the use of a digital logic bitwise XOR gate function, these characters were encrypted. A single binary-coded key performs this XOR operation on every character. For encryption and decryption of the entire information or data, keys were also repeated. The following equation denotes the encryption operation performed in the CXE algorithm. Equation numbered from (2)-(5) refers to the encryption of real data.

R_1 = XORed output of Element 0. i.e., 6517;
K_1 = random number generated by x_{n+1}

$$EK_1\ (R_1) = F_1 \tag{2}$$

R_2 = XORed result of Element 1. i.e., 3354;
K_2 = random number generated by x_{n+1}

$$EK_2\ (R_2) = F_2 \tag{3}$$

R_3 = XORed result of Element 2. i.e., C636;
K_3 = random number generated by x_{n+1}

$$EK_3\ (R_3) = F_3 \tag{4}$$

R_4 = XORed result of Element 3. i.e., 8456;
K_4 = random number generated by x_{n+1}

$$EK_4\ (R_4) = F_4 \tag{5}$$

Where d value ranges from 1 to j.

1.2.3 The Process of Decryption Process

While using reverse method of the encryption technique, the cipher texts were decrypted (transformed to plain text): The decryption of real data are denoted in Equation numbered from (6)-(8).

$$R_1 = DK_1\ (F_1) \tag{6}$$

Through decrypting Element 0 of the data received, R_1 is defined.

$$R_2 = DK_2\ (F_2) \tag{7}$$

Through decrypting Element 1 of the data received, R_2 is defined.

$$\ldots$$

$$R_4 = DK_4\ (F_4) \tag{8}$$

1.2.4 Key Generation Algorithm

Choose the parameter values.

As indicated in equation 2, using the logistic map equation, the pseudo-random numbers was generated.

Apply the BASE + XOR encoded result on these pseudo-random numbers and these numbers are generated from x_{n+1} to generate the keys k$_1$, k$_2$...k$_4$.

Then, keys in x_{n+1} are shifted to binary form which is 8 bit.

1.2.5 Encryption

Each element in Base + XOR is considered as R$_i$ which is represented in an 8-bit binary form.

EK_d (R$_i$) = Fi for all i>0, and d =1 to j.

In above condition, EK_d (R$_i$) denotes a bitwise XOR operation performed using one key K_d on real data.

The encryption process are shown from equation 2 to 5.

1.2.6 Decryption

R$_i$ = $DK_d\ (F_i)$ for all i>0 and d=1 to j.

In above condition, $DK_d\ (F_i)$ denotes a bitwise XOR operation performed using one key K_d on fake data.

The decryption process are shown from equation 6 to 8.

R$_i$ denotes Real data and it is mentioned in UNICODE which relates its decimal format.

Hence, character i denotes the UNICODE of R$_i$.

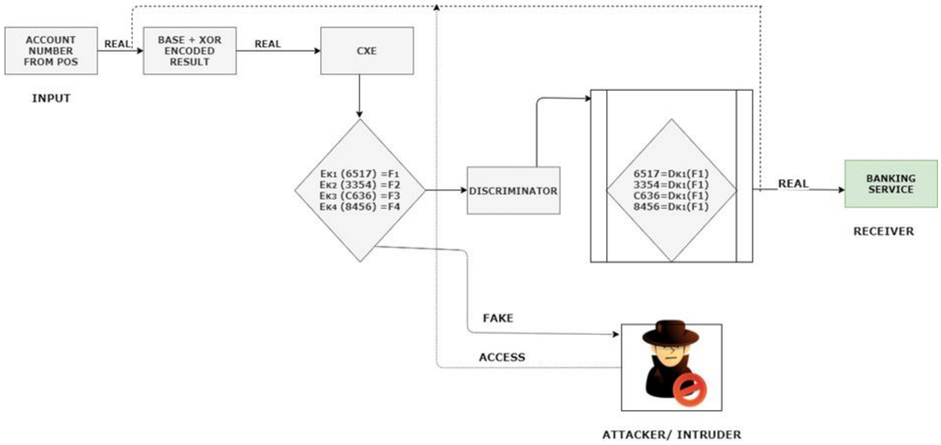

Figure 4: The process of the CXE technique

Figure 4 displays the process of the CXE technique. This technique is used to increase the security of banking data. First, from the POS terminal the real data is obtained and then encoding is proceeded with BASE + XOR. This process is previously described in section 3.1. In the CXE technique, instead of bank data, the BASE +XOR result is taken as input, and the encoding is performed. Thereafter, the encoded data is transformed to the discriminator. The discriminator performs the decoding process which is similar to encoding. Finally, the real data from POS is sent to the banking service and fake data from CXE is send to the attacker while accessing the data. This proposed technique meets the neccesity of banking networks. This is not only needed for banking application and it alos required for all other domains which need very fast transmission and security simultaneously.

4. Result and Discussion

5.

Three parameters were used to compare the proposed with existing algorithms which are data transmission speed, average energy consumption, and throughput.

1.3 Data transmission

Table 4: Data transmission time between BASE+XOR and one-hot encoding

DATASET	DATA TRANSMISSION TIME (ms)

	BASE + XOR	**ONE HOT ENCODING**
1GB	0.2	1
5GB	1	2.1
10GB	2.4	3
20GB	3.2	3.8
50GB	4	4.7

In table 4 contains the data transmission values in milliseconds (ms) which are compared between BASE+XOR and one hot encoding technique. These values are based on the dataset.

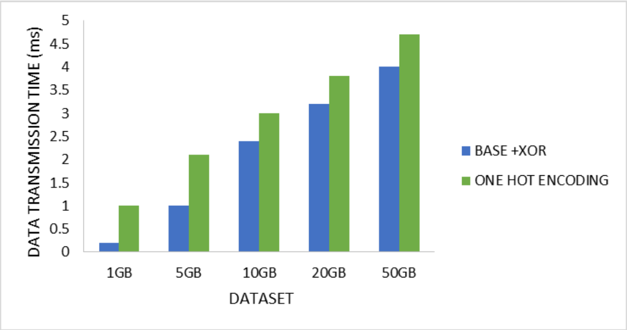

Figure 5: comparison of data transfer time values

Figure 5 shows, the comparison between BASE + XOR and one hot encoding technique. The BASE + XOR achieves small transfer time when compared to one-hot encoding at every dataset. Since it takes less time to calculate the encoding process, so the transfer time of the data set is low in the BASE+XOR technique.

1.4 Average energy consumption

Table 5: Average energy consumption between generator & discriminator and binary encoding

NUMBER OF NODES	**AVERAGE ENERGY CONSUMPTION [joules]**	
	GAN	**BINARY ENCODING**
15	0.4	1
30	1.2	1.8
45	2.3	3
60	3.2	3.7
75	4	4.5

In table 5 contains the energy consumption values in joules which are compared between GAN and binary encoding techniques. These values are based on the number of nodes.

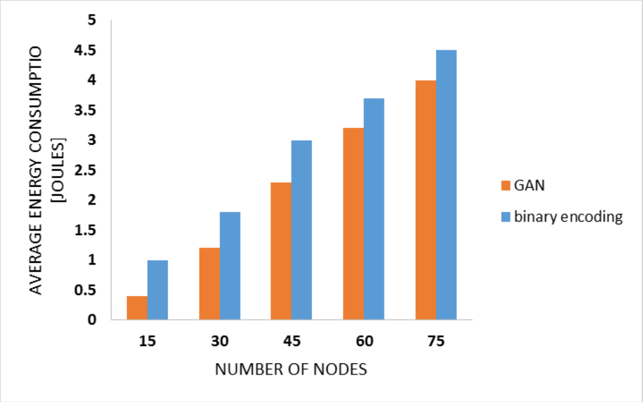

Figure 6: comparison of average energy consumption values

Figure 6 shows, the comparison between GAN and binary encoding techniques. The GAN has low energy consumption than binary encoding. The GAN passes the generator and produces fake data for security but the binary encoding has a long process of encoding for secured data.

1.5 Throughput

Table 6: Throughput between the CGAN and CNN

DATASET	THROUGHPUT [kb/sec]	
	CGAN	CNN
1GB	100	50
5GB	150	100
10GB	200	175
20GB	275	210
50GB	300	250

In table 6 contains the throughput values in kilobytes per second which are compared between CGAN and CNN techniques. These values are based on the dataset.

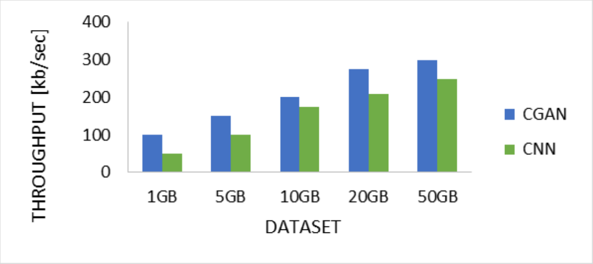

Figure 7: comparison of throughput values

Figure 7 illustrates the comparison of CGAN with CNN algorithms. The CGAN increases the throughput level when compared to CNN. The CGAN is the main role to perform between generator and discriminator and also it is used to secure data transmission.

1.6 Encryption time

Table 7: Encryption time

Data size in kb	Encryption time in seconds		
	AES	Chaotic Algorithm	CXE
200	1.23	1.10	0.0698
250	1.76	1.34	0.076

300	2.45	1.67	0.082
350	3.67	2.43	0.0891
400	4.23	2.68	0.0976
450	4.76	3.29	0.1053

Table 7 contains the encryption time value in seconds which are compared between AES, Chaotic, and CXE.

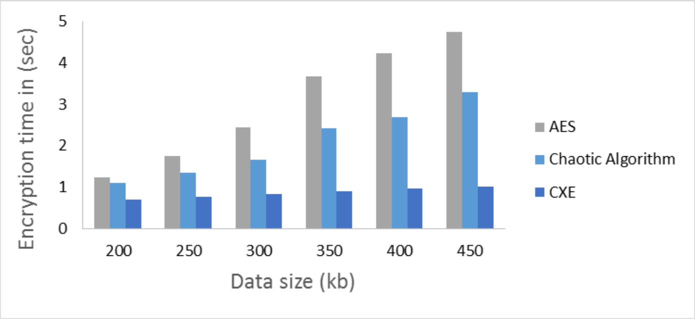

Figure 8: Comparison of encryption time between encryption algorithms

The proposed algorithm CXE is shown in Figure 8 and the comparison is between AES encryption and the Chaotic Algorithm. The proposed approach works much better for different message sizes which ranges from 200 KB to 450 KB. CXE can be applied for huge data sizes and with low encryption time.

6. Conclusions

Security and cost are the two major issues in data transmission in IoT. This work solved these major problems by two techniques such as BASE+XOR and CXE encoding mechanisms. BASE+XOR encoding mechanism is used to encode the real data which is transferred from POS. Following this, the data is encoded again using the CXE technique. The final encoded result is transferred to the discriminator. Discriminator splits the real data and encoded data after processing. Finally, real data is sent to the banking service and fake data (encoded data) is send to the attacker when they attack the real data. The BASE+XOR and CXE techniques are implemented effectively for security and lightweight data transmission. Especially CXE technique is proved to be faster as well as stronger than other encryption algorithms.

7. Future Work

In near future, the advanced encryption which is a fully homomorphic encryption technique will be proposed. It performs the arithmetic operations on ciphertext to ensure data privacy.

8. Acknowledgments

The author would like to appreciate the effort of the editors and reviewers. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

A. [Farooq Shaikh, 19] Farooq Shaikh and Elias Bou-Harb.: IoT Threat Detection Leveraging Network Statistics and GAN: 2019.

B. [Hao Ye, 18] Hao Ye, Geoffrey Ye Li, and Ling-Hwang Fred Juang.: Channel Agnostic End-to-End Learning-based Communication Systems with Conditional GAN: IEEE Globecom Workshops (GC Wkshps), 2018.

C. [Remah a. Alshinina, 18] Remah a. Alshinina & khaled m. elleithy.: A Highly Accurate Deep Learning Based Approach for Developing Wireless Sensor Network Middleware: IEEE.

D. [Zhaoqing Pan, 19] Zhaoqing Pan, Weijie Yu, Xiaokai Yi, Asifullah Khan, Feng Yuan, and Yuhui Zheng. : Recent Progress on Generative Adversarial Networks (GANs): A Survey: IEEE Access, 2019, Vol.7.

E. [Xiaopu Zhang, 19] Xiaopu Zhang, Shuai Zhan, Jun Lin, Feng Sun, Xi Zhu, Yang Yang, Xunqian Tong, And Hongyuan Yang. : An Efficient Seismic Data Acquisition Based on Compressed Sensing Architecture with Generative Adversarial Networks: IEEE access, 2019, Vol. 7.

F. [Decheng Wu, 20] Decheng Wu, Hailin Cao, Dian Li, And Shizhong Yang.: Energy-Efficient Reconstruction Method for Transmission Lines Galloping With Conditional Generative Adversarial Network: 2020, Vol.8.

G. [Zahangir Alom, 19] Md Zahangir Alom, Tarek M. Taha , Chris Yakopcic , Stefan Westberg , Paheding Sidike , Mst Shamima Nasrin , Mahmudul Hasan , Brian C. Van Essen , Abdul A. S. Awwal and Vijayan K. Asari.: A State-of-the-Art Survey on Deep Learning Theory and Architectures: MDPI, 2019.

H. [Akshay Mehrotra, 17] Akshay Mehrotra and Ambedkar Dukkipati.: Generative Adversarial Residual Pairwise Networks for One Shot Learning: Computer Vision and Pattern Recognition, 2017.

I. [Elhoseny, 19] M. Elhoseny & A. E. Hassanien.: secured data transmission in WSN: an overview: springer, 2019.

J. [Mohammed Aledhari, 17] Mohammed Aledhari, Marianne Di Pierro Mohamed Hefeida & Fahad Saeed 2017. : A Deep Learning-Based Data Minimization Algorithm for Fast and Secure Transfer of Big Genomic Datasets: IEEE transactions on big data, 2017.

K. [Bhavnesh, 19] Bhavnesh Jaint, S.Indu & Neeta Pandey.: Energy Efficient Communication Techniques for Wireless Sensor Networks: International Journal of Innovative Technology and Exploring Engineering, 2019.

L. [Bhanupriya, 17]1P. Bhanupriya, Shereen, Sylvia Blossom & Malathy.: Energy efficient wireless Sensor networks using raptor codes: International Journal of Advanced Research in Electronics and Communication Engineering, 2017.

M. [Donghyuk, 18]Donghyuk Lee, Mike O’Connor & Niladrish Chatterjee.: Reducing Data Transfer Energy by Exploiting Similarity within a Data Transaction: IEEE conference, 2018.

N. [Ankur, 15]Ankur Khare Piyush, Kumar Shukla, Murtaza Abbas Rizvi and Shalini Stalin .:An Intelligent and Fast Chaotic Encryption Using Digital Logic Circuits for Ad-Hoc and Ubiquitous Computing: MDPI, vol.18.

O. [Bassem, 13]Bassem Bakhache, Joseph M. Ghazal, and Safwan El Assad.: Improvement of the Security of ZigBee by a New Chaotic Algorithm: IEEE, 2013.

P. [Ramalingam, 19]H. Ramalingam and V. P. Venkatesan.: Conceptual analysis of Internet of Things use cases in banking domain: TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), 2019, pp. 2034-2039.

Q. [Jason Brownlee, 19]Jason Brownlee.: How to Develop a Conditional GAN (cGAN) From Scratch: July 2019, https://machinelearningmastery.com/how-to-develop-a-conditional-generative-adversarial-network-from-scratch/.