International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secured Data Transmission in IoT using Homomorphic Encryption

Suganya.S[1], Ramasamy.K[2], Dr. A. Srinivasan[3], Suba.M[4], Dr.V. Kalaichelvi[5], Swaminathan.S*[6]

[1,] Assistant professor Department of Information Technology, [2,4,6] Assistant professor, Department of ECE
[3]Associate professor, Department of ECE, [5] Associate professor, Department of CSE,
[1]

Submitted: 22/07/2022 **Accepted**: 25/09/2022

Abstract: The IoT systems transfer highly sensitive data in a network and majority of the people needs IoT technology in real time applications like smart home, smart health care etc., A number of security algorithms exists to protect the IoT systems but with some time complexity. Deep learning is considered to be an efficient technique to analyze threats and respond to attacks and security incidents instantly and accurately. Conditional Generative Adversarial Network (CGAN) is one of the deep learning technique that protects data based on conditions created by generator and discriminator models. CGANs are useful for getting features of choice in generated data. This work use the CGAN feasibility to controllable the data encryption and decryption part in GAN network. This work solve the time complexity issues using Algebraic Matrix in Conditional GAN (AMCGAN) and Fully Homomorphic Encryption (FHE) algorithm. The advantage of using algebraic matrix is to reduce the time complexity and input complexity in cryptography process. It performs both addition and multiplication at the same time, and can compute any operation instantly. There are many encryption techniques used to encrypt the data but the same time they have more time to decrypt the result. Because the mathematical evaluation are complex to derived in encryption part and otherwise. So, this work considered to address the time complexity problem by solving the easiest mathematical derivations in encryption and decryption part. Also we noticed that the fully homomorphic encryption algorithm have less encryption time compared to Chaotic Algorithm and it has minimal time complexity than existing algorithms such as RSA algorithm.

Keywords: *IOT systems, CGAN technology,*

1. Introduction

The Internet of Things (IoT) is the most recent and popular invention in recent years, allowing physical items to process and interact with virtual entities. Because all of the entities are interconnected, IoT makes it difficult to find, process, and analyse relevant data from the whole system. As a result, safeguarding confidential information from multiple attackers who gather, analyse, and transmit information of individuals to unauthorized persons (data consumers) seems to be more difficult. Personal data (any information related to a recognized or identifiable individual) is particularly attractive to data brokers or invaders because that could be useful to provide clients with significant services (Hyeontaek et al. 2019).

In order to identify known threats, network intrusion detection systems are generally rule-based and signature-based controls installed at the perimeter. Adversaries can readily defeat standard network detection mechanism by changing malware signatures. Self-taught learning-based deep learning systems have shown promise in identifying unexpected network breaches. Deep neural net-based solutions have been used to handle typical security concerns like malware identification and spyware identification. Deep learning is a multilevel nonlinear transformation-based hierarchical machine learning approach that excels in extracting raw data that transformed into abstract and generalized feature representations. Many issues that are deemed difficult in machine learning may be solved with deep learning. Deep learning recently developed considerable advancement in a variety of machine learning fields, owing to the development of large data and hardware acceleration (Fangchao et al. 2020). A generative adversarial network, or GAN is a deep learning-based generative model training architecture. The architecture is made up of a generator and a discriminator model. The generator model is for producing new plausible instances that are indistinguishable from the real samples in the dataset.

The discriminator method is for classifying data as real (derived from the dataset) or fake (generated). The conditional generative adversarial network (CGAN) is a kind of GAN that uses a generator model to conditionally generate data. If a class label is supplied, data production can be conditional on it, allowing for the focused generation of data of a specific type. Juan et al. (2019) presented a unique GAN-based method for preserving gender details while creating synthetic pictures. Within the conditional GAN method, it employs a latent vector to encode gender data.

Thiagarajan et al. (2018) described about the cryptographic algorithms. It protects data from cyber-attacks throughout encoding and decoding. They are expensive processes that use a lot of space and time of CPU during encoding and decoding. As a result, the objective of the project is to encode and decode messages using a key and a cyclic square matrix in a short amount of time. This method may be used for any number of words with a

[1] *A.V.C. College of Engineering, MannampandalMayiladuthurai,609001,india*
[2,3,4,5,6] *SRC,SASTRA DEEMED UNIVERSITY, Kumbakonam,612001,india*
** Corresponding Author Email: swaminathans@src.sastra.edu,*

larger amount of characters and the largest word.

Many encryption techniques have been introduced to protect such data from the intruders. The most popular technique is the FHE. Partially Homomorphic Encryption PHE, Fully Homomorphic Encryption FHE, and Somewhat Homomorphic Encryption SWHE, are the three primary types of homomorphic encryption methods. PHE systems, including as RSA, ElGamal, Paillier, and others, allow encrypted data to be added or multiplied. Fully homomorphic encryption may be used to create a scheme that supports both addition and multiplication at the same time. Fully homomorphic encryption can perform operations on encrypted data without violating users' privacy since the duration of the encryption results will be huge and the computation time of homomorphic multiplication and addition will be too long to be acceptable (Sarah & Ali 2018). As a result, according to the scope of the problem and the resources available, they must be leveraged. Furthermore, homomorphic matrix multiplication may be performed in parallel, significantly reducing computation time and mitigating this issue (Weiru et al. 2020). Thus FHE is considered in this work.

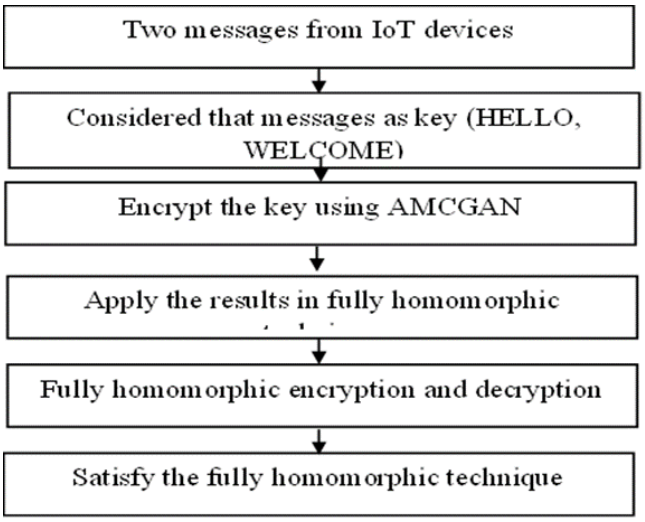

Fig 1: Flow diagram

IoT is rapidly getting popular among consumers all over the world, displacing traditional data transport methods. The volume of customer data entered in IOT systems has certainly become tempting targets for hackers, whether through illegal access, mobile malware, or compromising the backend. In recent years they are less encryption algorithm for handle the unauthorized access of information in IOT systems with less time complexity. Therefore, this work proposed the algebraic matrix encryption in conditional GAN (AMCGAN) to handle the unauthorized access of information in IoT system and also satisfy the homomorphic encryption technique with the help of algebraic matrix encryption result.

The Contribution of the proposed work :This work use the CGAN network for adding an extra encryption technique in generator using algebraic matrix to solve the time complexity issues in the encryption process. Moreover, encoded data is used as input for FHE. The purpose of using FHE to additionally protect the data from IoT. This work the messages from IoT are considered as key for encryption purpose.

2. Literature survey

Delu and Jianjun (2020) developed a unique reversible data concealing technique regarding a specific encryption procedure for encrypted data. The stream cypher and prediction error are integrated in the proposed particular encryption technique to save up space for data embedding. After that, the encrypted data is subjected to a permutation process to increase security.

Using Somewhat Homomorphic Encryption, Lizhi et al (2018) presented a encoded multimedia information and high-capacity reversible data hiding method. Three neighbouring pixels in an image are chosen as a group for the whole procedure. An image provider encrypts the original picture in the encryption section. The picture is then encrypted and transmitted to data hider. In the data concealing section, each group can get two absolute differences. By changing the histogram of absolute differences, the extra data is incorporated into the encrypted image.

Zhaoqing et al. (2019) discussed current advances in GANs. First, the core idea of GANs was examined and summarized, as well as the distinctions between various generative models. After that, the GANs' generated models are categorized, and training hints and assessment metrics are provided. The applications of GANs for performance enhancement were then described.

Xiaopu et al. (2019) suggested a framework for compressed sensing with a generative adversarial network (CSA-GAN) as an effective seismic data acquisition approach to overcome the limitations of gathering large scale seismic data. A data collecting architecture based on compressive sensing theory was used in the CSA-GAN to minimize the overall data traffic load and optimize transmission of data.

Decheng et al. (2020) presented CR-CGAN, a new curve reconstruction approach based on a conditional generative adversarial network (GAN), for completely synthesizing transmission line Galloping curves. They leveraged the recently announced GAN's modelling capabilities by applying extra restrictions to accomplish complete reconstruction of the galloping curves, as well as an unique generator-discriminator pair for enhanced outcome and a new improved loss function to increase the information.

Tushar et al (2017) proposed a transposition module named as Modified RSA for data encryption. This transposition component will receive the input and scramble and reorganize the information before passing it to RSA. The transposition's output will be placed into a modified RSA, which will create the encrypted text that will be sent over the network.

The conditional generative adversarial net (GAN) was introduced by Hao et al (2020) to describe The transmitter and receiver Deep Neural Networks (DNNs) are connected such that the gradient of the transmitter DNN may be back-propagated from the receiver DNN. The received signal related to the pilot symbols is given as part of the GAN's conditioning information, which is utilised to replicate the channel effects in a data-driven way.

By computing the greatest common divisor with the Euclidean technique, Wenju et al (2019) shown that, from the homomorphic computation key and a pair of known plaintext/ciphertext, the secret key may be obtained. The holy grail of cryptography, fully homomorphic encryption (FHE), allows for meaningful calculations on encrypted data.

Mohammed et al. (2017) propose a new deep learning-based data minimization algorithm that: 1) reduces datasets throughout carrier

channel transmission; and 2) prevents information from man-in-the-middle (MITM) or other attacks by changing the binary representation (content-encoding) so many times for the same dataset: they assign code words to the same character in various sections of the database.

Farooq Shaikh and Elias (2019) 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 relevant dataset of IoT devices and flagged malicious devices found deviating from their norm.

Akshay and Ambedkar (2017) suggested a deep residual network-inspired network architecture that enables the effective calculation of a more descriptive pairwise commonality purpose. They also suggested an additive generator network based on the Generative Adversarial Networks, where the discriminator is their residual pairwise network, arguing that regularization is crucial in learning with limited quantities of data.

3. Methodology

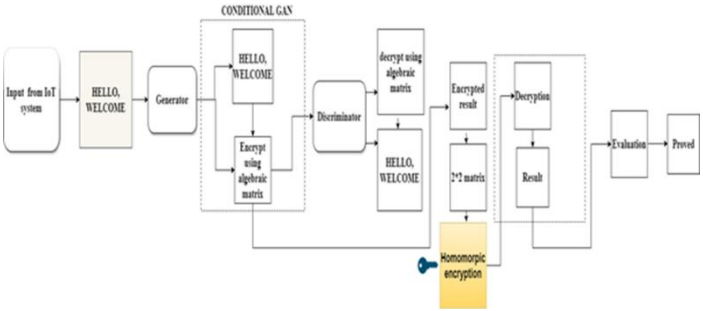

Fig 2: Architecture of the proposed work

3.1. Algebraic Matrix Encryption in Conditional GAN (AMCGAN)

Define abbreviations and acronyms the first time they are used in the text, even after they have already been defined in the abstract. Abbreviations such as IEEE, SI, ac, and dc do not have to be defined. Abbreviations that incorporate periods should not have spaces: write "C.N.R.S.," not "C. N. R. S." Do not use abbreviations in the title unless they are unavoidable (for example, "IEEE" in the title of this article). The proposed work use the CGAN network for running the major task. Generally, GAN doesn't contain the class of choice which means couldn't handle the controllable information in generator and discriminator. But CGAN provides that feasibility so this work choose the CGAN. Figure 2 represent the architecture of this proposed work where conditional GAN is represented in dotted line. In that process, the algebraic matrix function is used for encrypting the HELLO and WECOME messages, this task is done in generator of the CGAN. After that, similarly used the algebraic matrix for decryption. The encrypted result is an input for FHE. In general, FHE compute any operation like addition, multiplication etc. This work use the FHE for additional secure and reduce the time complexity for their mathematical evaluation.

3.1.1Encryption

Step 1: The Alphabets' value are assigned as A =-1, B =-2, ..., M =-13 and N=13, O=12, ..., Z=1.

A= -1	B = - 2	C= - 3	D= -4	E= -5	
F= -6	G= -7	H= -8	I= -9	J= -10	K= -11
L= -12	M= -13	N= 1	O= 2	P= 3	Q= 4
R= 5	S= 6	T= 7	U= 8	V= 9	W= 10
X= 11	Y= 12	Z= 13			

Step 2: Get the key for Encryption. Let the key be K_1 , K_2, ...,K_n where n is a number of words in the message.

Step 3: lets consider the messages are K_1 =HELLO, K_2 = WELCOME, use the step 1, allocate each character in K_1, K_2, ...,K_n to digits isolated by spacing between characters and words.

Key 1= HELLO

H= -8 E= -5 L= -12 L= -12 O= 2

Key 2= WELCOME

W= 10 E= -5 L= -12 C= - 3 O= 2 M= -13 E= -5

Step 4: Construct the Cyclic Square Matrix with characters in K_i for each i =1, 2,... n

K_1

-8	-5	-12	-12	10
-5	-12	-12	10	-8
-12	-12	10	-8	-5
-12	10	-8	-5	-12
10	-8	-5	-12	-12

K_2

4	-5	-12	-3	12	-13	-5
-5	-12	-3	12	-13	-5	4
-12	-3	12	-13	-5	4	-5
-3	12	-13	-5	4	-5	-12
12	-13	-5	4	-5	-12	-3
-13	-5	4	-5	-12	-3	12
-5	4	-5	-12	-3	12	-13

Step 5: Compute the amount of characters in a word, η (K_i) for each i =1, 2,..., n

Step 6: Calculate the E (η (K_1))

$$\begin{cases} W_i = \frac{j+1}{2} \text{ if } \eta(K_i) = j \text{ is odd}, k = 1, 2 \ldots . n \text{ and } I, j = 1, 2 \ldots \\ W_i = \frac{j}{2} \text{ if } \eta(K_i) = j \text{ is even}, k = 1, 2 \ldots . n \text{ and } I, j = 1, 2 \ldots \end{cases}$$

Then for $K_1$and, η (K_1) = 5, E (η (K_1)) = (5+1)/2 =3 and E η (K_2) = 7, E (η (K_2)) = (7+1)/2 = 4. Therefore E (η (K_1)) = 3rd implies that values of 3rd column along the word K_1 and E η (K_2) = 4 denotes that 4th column values along the keyK_2 .

Step 7: Assign each column value as matrices to b1 and b2 which is b1= -12 -1210-8-5 and b2= -3 12-13-54-5-12.

Step 9: Compute the diagonal matrix D (b_1) $-5I_5$ =D (-17 -17 5 -13 -10) and D (b_2) $-7I_7$ = D (-10 5 -20 -12 -3-12-19), where b_1 and b_2 are the diagonal matrix respectively. Hence the encrypted results are 17 -17 5 -13 -10, -10 5 -20 -12 -3-12-19.

3.1.2 Decryption

Step 10: now, decrypt the K_1 and K_2 with the help of diagonal matrix. c_1= D (b_1) + 5I_5 =D (-12 -12 10 -8 -5) and c2= D (b_2) + 7I_7 = D (-3 12 -13 -5 4 -5 -12), where b_1 and b_2 are the diagonal matrix respectively. Hence the decrypted results are-12 -12 10 -8 -5, -3 12 -13 -5 4 -5 -12.

Step 11: use the step 6 compute the n (b_1) =E (η (b_1)) and n (b_2) = E (η (b_2)). Thus n ($\underline{b_1}$) = 3 denotes that the first digit of b_1 is the 3rd character of the first word of the decrypted key and n (b_2) = 4 denotes that the first digit of b_2 is the 4th character of the second word of the decrypted key.

Step 12: let c_1 = -12 -12 10 -8 -5 → 3rd 4th 5th 1st 2nd , now rearrange the values from 1st to 5th , -8 -5 -12 -12 10 which is HELLO.

c_2 = -3 12 -13 -5 4 -5 -12 → 4th 5th 6th 7th 1st 2nd 3rd. Now rearrange the values from 1st to 7th, 4 -5 -12 -3 12 -13 -5 which is WELCOME.

The sample (-12 -12 10 -8 -5) encrypt result is used as input to FHE for additional security. The HELLO is encrypt by 12 -12 10 -8 -5 and used this encrypt value for 2 by 2 matrix operation in FHE that is done in generator of the CGAN and similarly decryption part is completed in discriminator of the CGAN.

3.2. Satisfy the fully homomorphic encryption technique

Use one space after periods and colons. Hyphenate complex modifiers: "zero-field-cooled magnetization." Avoid dangling participles, such as, "Using (1), the potential was calculated." [It is not clear who or what used (1).] Write instead, "The potential was calculated by using (1)," or "Using (1), we calculated the potential."

Use a zero before decimal points: "0.25," not ".25." Use "cm^3," not "cc." Indicate sample dimensions as "0.1 cm × 0.2 cm," not "0.1 × 0.2 cm^2." The abbreviation for "seconds" is "s," not "sec." Use "Wb/m^2" or "webers per square meter," not "webers/m^2." When expressing a range of values, write "7 to 9" or "7-9," not "7~9."

A parenthetical statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.) In American English, periods and commas are within quotation marks, like "this period." Other punctuation is "outside"! Avoid contractions; for example, write "do not" instead of "don't." The serial comma is preferred: "A, B, and C" instead of "A, B and C."

If you wish, you may write in the first person singular or plural and use the active voice ("I observed that ..." or "We observed that ..." instead of "It was observed that ..."). Remember to check spelling. If your native language is not English, please get a native English-speaking colleague to carefully proofread your paper. Homomorphic encryption is a sort of encryption that enables individuals to compute on encoded information without having to decode it first. Fully homomorphic encryption (FHE) is a form of homomorphic encryption that allows analytical processes to be run directly on encrypted data while still producing the same encrypted outputs as if they were performed on plaintext. This work used the FHE for reducing the encryption time complexity with their evaluation. Because FHE run its performance directly on encrypt data so the time will be reduced.

FHE performs both addition and multiplication at the same time, and can compute any operation. In recent pasts, there are many encryption algorithms used to convert the cipher text to plain text and vice versa, but still they are not efficient and easiest method to convert the texts or data, because that contains the set of complex mathematical formulas which takes more number of time to process. This work overcome the complexity issue using algebraic matrix result to proof the homomorphic encryption technique. The following subsections like key generation, encryption, decryption and evaluation to describe the FHE equation part.

3.2.1 Key generation

Step 1: Let consider the HELLO key and WELCOME key which is already encrypted using algebraic matrix and again it is used to encrypt by fully homomorphic technique.

Step 2: The encrypted n value of HELLO key is (n= 3) and otherwise decrypted (m=3). Select another number as u and this work consider the u value as (-12, -12, 10, -8, -5) get from the algebraic matrix encrypted result.

Step 3: set the 2 by 2 matrix condition in generator.

Step 4: arrange the u values where, u= $\begin{bmatrix} -12 & -12 \\ 10 & -8 \end{bmatrix}\begin{bmatrix} -5 & 0 \\ 0 & 0 \end{bmatrix}$

u =$\lfloor 96 + 120 \rfloor$ = 126

u = 126

Now, calculate the S = n*u

S =3 * 216

S= 648

Step 5: Select the random big integer t= 8 and apply the computed values to formula.

e= t (n-m +1)

e= t (3-3+1)

e =8 (1)

e=8

Public key (e, s) = (8, 648)

Secret key (n) = 3

3.2.2 Encryption

Select the two random integer r_1= 5 and r_2 =3 and two message M_1= 2 and M_2=1< n

Now calculate the C_1,

C_1=$M_1^{r1*e+1} mod$ s

= 2^{5*8+1}mod 648

= 2^{41}mod 648

C_1= 464

Then calculate the C_2,

C_2=$M_2^{r2*e+1} mod$ s

= 2^{3*8+1}mod 648

= 1^{25}mod 648

C_2= 1

3.2.3 Decryption

D_1=C_1 mod n

= 464 mod 3

D_1= 2

D_2=C_2 mod n

= 1 mod 3

D_2= 1

3.2.4 Evaluation

C_3= C_1 + C_2

= 464 + 1

C_3 = 465

C_4= C_1 * C_2

= 464* 1

C_4 = 464

Now decrypt of C_3,

D_3 =C_3 mod n

= 465 mod n

D_3 = 0

D_4 =C_4 mod n

= 464 mod 3

D_4= 2

Let C=[$((C_1 \ldots C_i)$]such as

C=[$((C_1 * C_3 + C_2) * C_4$]mod n

=[$((464 * 465 + 1) * 464]$ mod 3

= 100113104 mod 3

= 2

Let M=[$((M_1 \ldots M_i)$]such as

M=[$((M_1 * M_3 + M_2) * M_4$]mod n

=[$((2 * 0 + 1) * 2]$ mod 3

= 2 mod 3

= 2 = C (proved)

After finishing the encryption and decryption task, the evaluation part validate both the tasks. In evaluation task, the cipher text C_3 and C_4 is calculated by addition and multiplication and decrypt the cipher text D_3 and D_4 is calculated by mod operation. After that cross validation process is performed to measure the cipher text c and plain text m. Finally, C and M texts are proved which means the message reached securely to the receiver or server when using the FHE. So, the condition is satisfied.

separate compound units, e.g., "A·m^2."

The execution time of a given process is defined as the spent time on executing that process by the system, including the spent time on its behalf performing runtime. The mechanism used to measure implementation time is defined by execution.

Table 1: Comparison of the execution time

Size of the key	Execution time (m.s)		
	Elgamal	**RSA**	**AMCGAN**
12 byte	1600	1842	1985
1k byte	10291	11431	11472
1.5 k byte	21397	31321	41333
2 k byte	34112	40310	53121
2.5 k byte	59863	61313	73403

In Table 2: consider the five size of the key begin with (12 byte) and end with (2.5 K Byte) and to calculate the execution time between Elgamal, RSA Cryptosystems and AMCGAN.

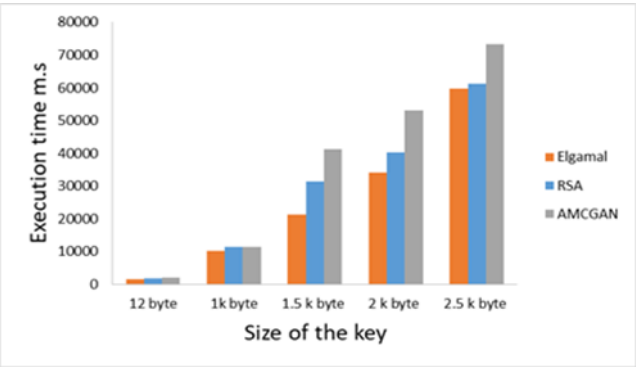

Figure 3: Comparison of the execution time

Figure 3 shows the AMCGAN executes less time than Elgamal and RSA encryption algorithm. Because AMCGAN calculate the diagonal matrix for encryption which helps to easiest method for decryption result also.

Table 2: Comparison of the Encryption time

Data size in kb	Encryption time in seconds		
	AES	**Chaotic Algorithm**	**Fully homomorphic**
200	1.23	1.10	0.069
250	1.76	1.34	1.23
300	2.45	1.67	1.54
350	3.67	2.43	2.23
400	4.23	2.68	2.47
450	4.76	3.29	2.65

Table 2 contains the encryption time value in seconds which are compared between AES, Chaotic, and fully homomorphic.

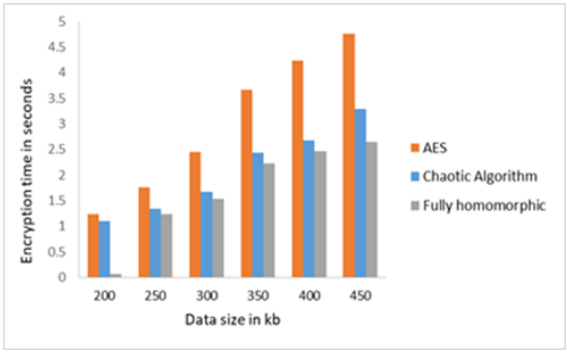

Figure 4: Comparison of the Encryption time

Figure 4 shows the fully homomorphic is much faster when it is compared to AES encryption and the Chaotic Algorithm. Because fully homomorphic algorithm provides the easiest arithmetic operation on encryption. The multiple message sizes from 200 KB to 450 KB is used to measure the optimized algorithm.

Table 3: Comparison of time complexity

DATASET	Time complexity [kb/sec]	
	CGAN	**AMCGAN**
1GB	100	50
5GB	150	100
10GB	200	175
20GB	275	210
50GB	300	250

In table 3 contains the throughput values in kilobytes per second which are compared between CGAN and **AMCGAN** techniques.

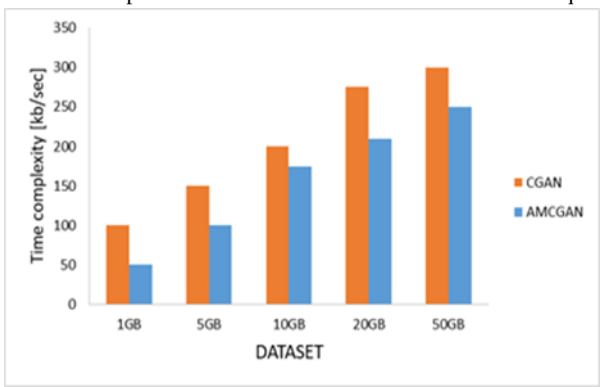

Figure 5: Comparison of time complexity

Figure 5 shows the AMCGAN is take less time to handle the

different size of dataset then CGAN. Because AMCGAN handle the encryption with the less time using diagonal matrix operations and also take this result as input for satisfy the fully homomorphic encryption algorithm with certain time. So the time complexity is reduced while the number of dataset is high.

4. Conclusion

. Time complexity is one of the major issues in IoT systems. This work solved these major problem by AMCGAN. The AMCGAN is used to encode the two messages from IoT systems. This work considered that messages are key it is encoded by the diagonal matrix in generator with certain condition. After encoded the messages which are transferred to the discriminator. Discriminator process the decoding operations. After decoded, the fully homomorphic is satisfied, if any unauthorized person or intruder access the key, the encrypted result will be send.. The implementation time of the AMCGAN was faster than the Elgamal, RSA cryptosystems execution time. In comparison with AES and the Chaotic Algorithm, encryption time is reduced in homomorphic encryption algorithm. Finally, the overall time complexity is reduced in this work.

5.References

[1] Hyeontaek Oh Gyu Myoung Lee, Sangdon Park And Jun Kyun Choi Hwanjo Heo), "Personal Data Trading Scheme for Data Brokers in IoT Data Marketplaces", IEEE Access. 2019

[2] Fangchao YuLi WangXianjin FangYouwen Zhang , "The Defense of Adversarial Example with Conditional Generative Adversarial Networks", Security and Communication Networks.2020

[3] Juan E. Tapia, Claudia , "ArellanoSoft-biometrics encoding conditional GAN for synthesis of NIR periocular images", Future Generation Computer Systems.2019

[4] Bulla, P. . "Traffic Sign Detection and Recognition Based on Convolutional Neural Network". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 43-53, doi:10.17762/ijritcc.v10i4.5533.

[5] Vanitha, D. D. . (2022). Comparative Analysis of Power switches MOFET and IGBT Used in Power Applications. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 01–09. https://doi.org/10.17762/ijrmee.v9i5.368

[6] K Thiagarajan, P Balasubramanian, J Nagaraj, J Padmashree "Encryption and decryption algorithm using algebraic matrix approach", IOP Conf. Series: Journal of Physics: Conf. Series 1000.2018

[7] Sarah Shihab Hamad, Ali Makki Sagheer "Public Key Fully Homomorphic Encryption", Journal of Theoretical and Applied Information Technology 96(7), 1924-1934.2018

[8] Weiru Wang, Yanfen Gan, Chi-Man Vong, Chuangquan Chen "Homo-ELM: fully homomorphic extreme learning machine",. Int. J. Mach. Learn. & Cyber, 11, 1531–1540.2020

[9] Delu Huang, Jianjun Wang , "High-capacity reversible data hiding in encrypted image based on specific encryption process", Signal Processing: Image Communication, 80.2020

[10] Lizhi Xiong, Danping Dong, Zhihua Xia And Xianyi Chen , "High-Capacity Reversible Data Hiding for Encrypted Multimedia Data With Somewhat Homomorphic Encryption", IEEE Access, vol. 6, pp. 60635-60644.2018

[11] Zhaoqing Pan, Weijie Yu, Xiaokai Yi, Asifullah Khan, Feng Yuan, and Yuhui Zheng Recent Progress on Generative Adversarial Networks (GANs): A Survey: IEEE Access, Vol.7.2019

[12] Ahmed Cherif Megri, Sameer Hamoush, Ismail Zayd Megri, Yao Yu. (2021). Advanced Manufacturing Online STEM Education Pipeline for Early-College and High School Students. Journal of Online Engineering Education, 12(2), 01–06. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/47

[13] Singh, S. . (2022). Unconditionally G ?odel Degeneracy for Quasi-Meager, Smooth Moduli. International Journal on Recent Trends in Life Science and Mathematics, 9(1), 28–36. https://doi.org/10.17762/ijlsm.v9i1.139

[14] Baes, A. M. M. ., Adoptante, A. J. M. ., Catilo, J. C. A. ., Lucero, P. K. L. ., Peralta, J. F. P., & de Ocampo, A. L. P. (2022). A Novel Screening Tool System for Depressive Disorders using Social Media and Artificial Neural Network. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 116–121. https://doi.org/10.18201/ijisae.2022.274

[15] 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, Vol. 7.2019

[16] Ghazaly, N. M. . (2022). Data Catalogue Approaches, Implementation and Adoption: A Study of Purpose of Data Catalogue. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 01–04. https://doi.org/10.17762/ijfrcsce.v8i1.2063

[17] Decheng Wu, Hailin Cao, Dian Li, And Shizhong Yang , "Energy-Efficient Reconstruction Method for Transmission Lines Galloping With Conditional Generative Adversarial Network", IEEE Access, vol. 8, pp. 17310-17319.2020

[18] Tushar Vyavahare, Darshana Tekade, Saurabh Nayak, N Suresh kumar and S S Blessy Trencia Lincy , "Enhanced rearrangement technique for secure data transmission: case study credit card process", IOP Conf. Series: Materials Science and Engineering, 263 (4).2019

[19] Hao Ye, Le Liang, Member, Geoffrey Ye Li, Fellow, and Biing-Hwang Juang , "Deep Learning-Based End-to-End Wireless Communication Systems with Conditional GANs as Unknown Channels", IEEE Transactions on Wireless Communications, Vol. 19, No. 5.2020

[20] Enju Xu, Yu Zhan, Zheng Wang, Baocang Wang And Yuan Ping , "Attack and Improvement on a Symmetric Fully Homomorphic Encryption Scheme", IEEE Access. vol. 7, pp. 68373-68379,2019

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

[22] Farooq Shaikh and Elias Bou-Harb , "IoT Threat Detection Leveraging Network Statistics and GAN.2019

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

[24] Swaminathan.s, Ramasamy.k, Srinivasan.A, AB2IG – an Efficient Crypto System, ,Far East Journal off Electronics and Communications 16:171-78,DOI:10.17654/EC03010171, April 2016

[25] S. Swaminathan;A. Karthick;S. Suganya, A secure and robust crypto system based on unique dynamic key generation scheme, Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT),IEEE,Year: 2014