Traitement du Signal
Vol. 41, No. 1, February, 2024, pp. 401-410
Journal homepage: http://iieta.org/journals/ts

Enhancing Secure Data Transmission in IoT via Advanced Conditional Generative Adversarial Network and Encryption Techniques

Gopu A. Palanisamy[1*], Sivaraj Rajappan[2], Vijayakumar Murugasamy[3]

[1] Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Thindal, Erode 638012, Tamil Nadu, India
[2] Department of Computer Science & Engineering, Nandha Engineering College, Perundurai, Erode 638052, Tamil Nadu, India
[3] Department of Computer Science & Engineering, Sasurie College of Engineering, Vijayamangalam, Tirupur 638056, Tamil Nadu, India

Corresponding Author Email: gopumecse@gmail.com

https://doi.org/10.18280/ts.410134

Received: 18 May 2023
Revised: 1 August 2023
Accepted: 8 September 2023
Available online: 29 February 2024

Keywords:
Algebraic Matrix Encryption, data transmission, deep learning, Fully Homomorphic Encryption, Generative Adversarial Network, Jaro-Winkler similarity

ABSTRACT

Addressing the challenge of secure data transmission within the Internet of Things (IoT) necessitates robust solutions. Deep learning has emerged as a potent tool for threat analysis and response to security incidents in the IoT landscape. A particular method, namely the Generative Adversarial Network (GAN), is utilized for identifying attacks during secure data transmission. Despite its usefulness, GANs are not devoid of shortcomings, such as mode collapse, which limits the diversity of the generator's output. This issue often arises from training difficulties when the generator encounters a specific type of data that easily deceives the discriminator. To mitigate these limitations, this study introduces an enhanced model of the GAN, the Conditional GAN (CGAN), featuring two generators and two discriminators (G1, G2, and D1, D2). This model, when amalgamated with cryptographic techniques, effectively addresses the mode collapse issue. Furthermore, Algebraic Matrix Encryption (AME) and Improved Fully Homomorphic Encryption (FHE) algorithms are proposed as secure data transmission solutions. To evaluate the diversity of the generated fake samples, the Jaro-Winkler similarity measure is employed. A comprehensive comparison of the proposed model's efficiency is conducted, incorporating metrics such as Jaro-Winkler accuracy test, training time, loss, Root Mean Square Error (RMSE), Mean Absolute Error (MAE), Percent Root Mean Square Difference (PRD), recall, F-score, mean, and standard deviation. According to the analysis, the proposed model surpasses the performance of AEGAN and MTC-GAN, thereby demonstrating its potential in enhancing secure data transmission in IoT.

1. INTRODUCTION

Security remains a compelling challenge for both individuals and organizations, demanding thorough scrutiny at every stage, from initial design to daily operations. The lifecycle of a device necessitates rigorous security control, encompassing initial booting, patch updates, and all intermediate stages. The issue of IoT security becomes particularly critical during financial transactions or when handling private and confidential information. Given the ease of access to monitor data feeds, change settings, and modify authorizations, potential infiltrators have significant advantages [1].

Deep Learning (DL), with its increasing application across sectors such as healthcare and cybersecurity, is a potent tool for understanding 'normal' and 'abnormal' behaviors in the way IoT components and devices communicate within an IoT framework [2, 3]. By analyzing every input data component of the IoT system, common patterns of interaction can be identified, enabling early detection of malicious activity. Furthermore, ML/DL techniques can be instrumental in predicting new attacks, which are often adaptations of previous ones, as these techniques can effectively anticipate future unknown attacks by learning from existing ones [4]. To provide effective and secure solutions, IoT systems must progress beyond merely enabling secure device connectivity to offering security-based intelligence underpinned by DL/ML approaches.

Recent advancements in deep learning, such as Generative Adversarial Networks (GANs), can generate new data mirroring the statistical properties of the training set. For instance, a GAN trained on images can create new, seemingly realistic images. This implies that within an IoT setup, fake data can be integrated with the original message in the GAN to mislead an attacker with decoy information. However, these cross-modal translation frameworks prove inadequate for multi-domain image-to-image translation [5]. Existing cryptographic systems utilizing neural networks and generative adversarial neural networks have limited mechanisms for data security. Data anonymization, although a viable approach, does not guarantee complete data security, as some aspects of the protected data can still be inferred from the non-anonymised data [6].

Homomorphic encryption, a relatively recent and promising technique, can address cryptography-related challenges in AI. Accordingly, the current study aims to enhance GAN's architecture by incorporating two generators (G1 and G2) and two discriminators (D1 and D2). The contributions of this work are as follows:

- The work employs CGAN, introducing additional coding technology to the generator using an algebraic matrix to address time complexity issues in the coding process.
- A novel technique, termed Improved CGAN, is proposed to distinguish between real and fake data, ensuring secure data transmission.
- Encoded data serve as input for Fully Homomorphic Encryption (FHE), further bolstering the security of IoT data. IoT messages are crucial for cryptographic purposes within this project.
- The Jaro-Winkler similarity measure is used to assess the diversity of generated fake data.
- Conditional information (alphabets and numbers) is added to noise and used in the encryption process. The key sizes, derived from noise, are encrypted using an improved FHE in the second generator.

2. LITERATURE REVIEW

Previous research has explored the use of GAN-based models for detecting risks in IoT devices both within and outside the network. Some researchers have factored in the role of network function virtualization in managing hostile devices identified on the network [7]. Their GAN-based model identified malicious devices deviating from the norm by mapping the latent space of the relevant IoT device dataset.

In terms of data acquisition, an efficient seismic data acquisition approach known as the Compact Detection Framework with Generative Adversarial Network (CSA-GAN) was developed to address the limitations of large-scale seismic data acquisition. This approach relies on a data gathering architecture centered around compressed sensing theory, which reduces overall data traffic load and balances data transfer [8].

A novel strategy to handle mode collapse in GANs was developed using two discriminators. Although the use of two discriminators is not new, it has proven to be effective in overcoming some of GAN's inherent weaknesses [9]. The strategy effectively integrates the Kullback-Leibler (KL) and reversed KL divergences into a unified objective function, enabling it to efficiently vary the predicted density in collecting multi-modes [10].

In the realm of music, a novel melody composition approach was developed based on individual bars. This approach improved upon the original GAN model by creating a new GAN model with two discriminators: an LSTM model and a model ensuring bar correlation. This resulted in a reduction in the overall architecture's execution time compared to the traditional GAN [11].

Researchers have also proposed the Public Key Fully Homomorphic Encryption scheme (PKFHE), which is fundamentally based on Euler's theorem. This scheme proved to be faster in terms of temporal complexity and demonstrated strong data security in the cloud [12].

There has been research on verified public-key encryption with keyword search in a multi-user situation, using homomorphic encryption [13]. The researcher proposed a system based on the structure of the inverted encoding pointer and explained how it could be used to verify the accuracy and completeness of research results.

Another study proposed a faster FHE technique that required fewer ciphertext refreshes. This method, based on the Ducas and Micciancio (DM) technique, seemed to have a lower computational cost compared to the GSW and DM methods [14].

One of the latest innovations in privacy-preserving authentication techniques is homomorphic encryption [15]. This technology protects the privacy of users' data by ensuring that the results from homomorphic encryption processes are identical to those obtained from the original text.

A Conditional Activation GAN (CAGAN) was introduced to combine various GANs. The architecture of the integrated GANs had no significant influence on the number of computations [16]. Furthermore, to avoid batch normalization from ignoring the conditions specified in a CAGAN's discriminator.

In a bid to improve outcomes, a novel architecture in the generator-discriminator pair was presented along with a new refined loss function for improving details. The generator used an autoencoder with skip connections, and the inception module captured multiple scales of spatiotemporal correlation [17]. The refined loss function aimed to eliminate GAN artifacts and ensure better reconstruction performance.

To tackle both security and energy efficiency in IoT, two unique deep learning approaches were suggested [18]. The researchers proposed reducing the use of energy-intensive "1" values in the DRAM interface, thus offering an innovative power-saving solution in IoT devices. Furthermore, the data was protected by the chaotic XOR encryption (CXE) approach, which has been proved to be faster and more secure compared to XOR operation.

The proposed Variance Enforcing GAN (VARGAN) is a new GAN design that includes a third network to boost variety in generated data [19]. Due to its impressive diversity, low computational complexity, and fast convergence, VARGAN is a promising paradigm for preventing mode collapse.

The Dual Discriminator Weighted Mixture Generative Adversarial Network (D2WMGAN) approach demonstrated that it could effectively learn many modes of data, providing rich, realistic examples, and mitigate the issue of mode collapse [20].

An evolutionary multi-objective cyclic GAN (EMOCGAN) was suggested for solving the problem of mode collapse. However, there are a few limitations, such as when the proposed approach has a low UQI or is not comparable to the state-of-the-art [21].

The proposed attentive evolutionary generative adversarial network (AEGAN) approach was developed to resolve issues in existing GANs such as mode collapse, instability, and low processing efficiency [22].

By combining the strengths of the Variational Auto-Encoder (VAE) and the Generative Adversarial Network (GAN) with an auxiliary discriminative classifier network, researchers addressed the challenges of image blurriness and mode collapse to some extent [23].

Various encryption methods have been introduced to protect data from hackers. The most common technology is FHE. There are three main types of isomorphic encoding methods: Partially homomorphic PHE encoding, Somewhat Homomorphic SHE encoding, and Fully Homomorphic FHE encoding. The security of these encryption methods has been proven mathematically. However, FHE has a higher computational cost and requires more time to execute [24].

In conclusion, the literature review has shown that GANs have been used in various domains to generate data, including IoT, music, and seismic data. Despite their successful application in these fields, GANs still face issues such as mode collapse and high computational costs. Homomorphic encryption techniques, on the other hand, have proven to be secure but are also computationally expensive. Therefore, there seems to be a need for methods that can address these shortcomings.

3. METHODOLOGY

This section describes about proposed work in detail. The main objective of this work is to improve the GAN architecture for transferring the data securely and more efficiently in IoT applications and to solve the mode collapse problem. AME and improved FHE are used to encrypt and decrypt the IoT message.

The advantage of using an algebraic matrix is that the complexity involved in the encryption process was reduced. Though many techniques are used to overcome the mode collapse problem, still it is remaining as one of the challenging tasks in active research. This work utilized one additional generator and discriminator to handle the mode collapse problem in standard GAN.

3.1 Backgrounds of GAN

GAN is a generative model that allows two sub-models to compete for correct data generation. A GAN is made up of a generator and a discriminator. The generator's purpose is to create authentic fake data, whereas the discriminator's goal is to distinguish true data from the generator's fake data. Each of these models improves at their job during training, and the best stop state is a balancing act in which neither model outperforms the other. The generator extracts feature from the training data to generate realistic images. The discriminator is trained on its own to classify both the labeled false and real images. A GAN could get trapped in a few different failure scenarios. The two most common types of failures are convergence failure (which fails to produce good quality outputs), and mode collapse failure (which fails to create a variety of different-looking outcomes).

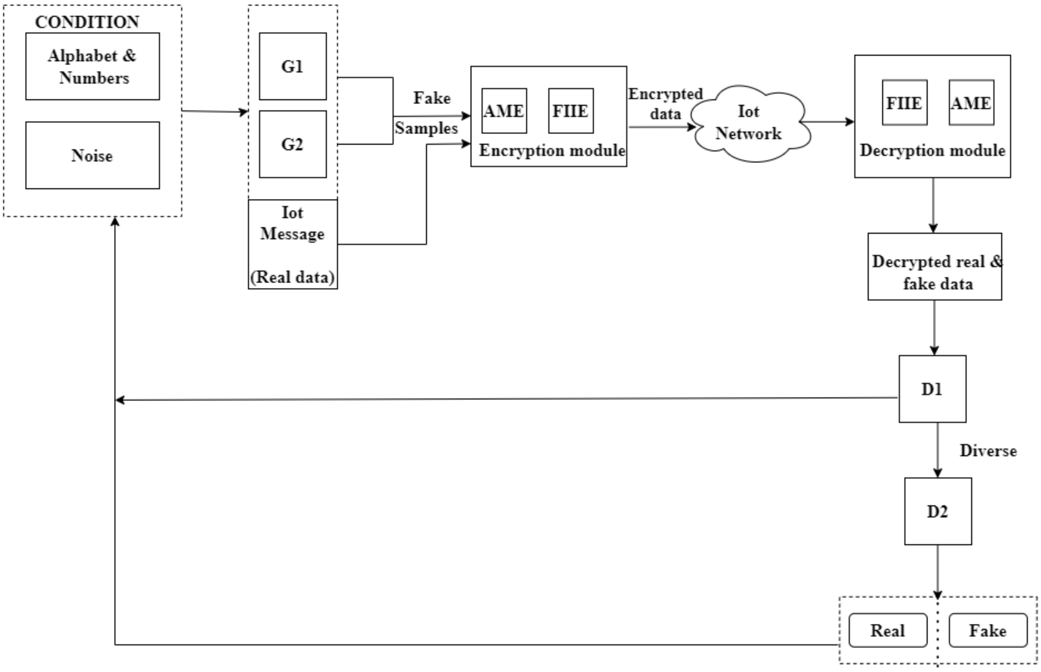


Figure 1. Architecture of proposed CGAN for secured data transmission

3.2 Problems in GAN

A well-trained GAN can typically produce a wide range of outputs. Whenever a generator could only generate a single output or a limited number of outputs, mode collapse occurs. This could be due to training issues, such as the generator discovering a type of data which can easily tricked the discriminator, then continues to generate that type. As the generator doesn't have an incentive to switch things up, the entire system will over-optimize on that one output. As a result, whether the data or any information is generated as accurate, the suggested study determined an additional generator and discriminator for identifying the mode collapse problem. This work solves the mode-collapse problem by monitoring whether the produced fake samples by the generators are diverse. If not, the feedback is given to solve this problem.

3.3 Improved CGAN

The proposed CGAN is improved with two generators (G^1 and G^2) and discriminators (D^1 and D^2) which solves mode collapse problem by checking whether the generated data samples by the generators are diverse in nature as well as similar to real data. Figure 1 depicts the proposed work's architecture. Initially, on the sender's side, the fake data samples generated by the generators (G^1 and G^2) and real samples are encrypted using AME and FHE techniques. It is further transmitted through IoT network to the receiver, where the received, data is decrypted using same two techniques (AME, FHE). Then, the discriminator (D^1) checks whether the generated samples are diverse. If so, then real and fake data are classified using discriminator D^2. Otherwise, the feedback is sent as a loss function to the generators. The FHE technique is improved to encrypt the message using the number of character counts in messages that are referred to as key size.

3.4 Dual generators

This work uses two generators G^1 and G^2. Both generate fake samples by taking noise and condition as input. The generators can be denoted as:

$$G_1(Y) = G_1^a(G_1^{a-1}\,(\ldots\ldots G_1^2\big(G_1^1(Y)\big))\big) \tag{1}$$

$$G_2(Y) = G_2^b(G_2^{b-1}\,(\ldots\ldots G_2^2\big(G_2^1(Y)\big))\big) \tag{2}$$

where, *a* and *b* denote the total number of layers in two generators. There can be single distribution for single generator and mixed distribution for two of them. In this work, we assume both generators have similar structure and same equal weights. Inspired from the work [22], this work uses feature matching loss for training the IoT data for mixed data distribution in generators. The feature matching loss function were utilized by generators to control the mixed data distribution, thereby reduces overlapping of high-density data regions of real data while remaining close to the genuine data distribution.

3.5 Dual discriminator

The receiver consists of dual discriminators D^1 and D$^{2.}$ In this, first one determines whether generated samples are diverse or not. For this, Jaro-Winkler similarity is used. If it is diverse, the next discriminator will classify the data as real and fake samples. Otherwise, feedback will be passed as loss function to the generators for improving the generated fake samples.

The two discriminators can be given as,

$$\begin{aligned} D_1(z_1) &= D_1^c(D_1^{c-1}\left(\ldots\ldots D_1^2\big(D_1^1(z_1)\big))\right) \\ &= D_2^e(D_2^{e-1}\left(\ldots\ldots D_2^2\big(D_2^1(z_2)\big))\right) \end{aligned} \tag{3}$$

In above equation, c and e refers to number of layers in two discriminators. First discriminator will find whether the generated samples are diversified or not. In the next step, discriminator 2 will classify samples as real and fake. In this work, we consider both discriminators share equal layers and weights to avoid mode collapse problem. This also reduces the number of parameters in receiver side.

3.6 Model training

The proposed model is based on data that have been trained using joint data distributions. Weight-sharing restrictions are a crucial component of our contribution since they allow networks to manage their shared data and boost efficiency. Furthermore, the sharing weight restriction permits the model to reduce the number of parameters while reducing the original GAN's complexity. Also, this work assumes the generators and discriminators share same number of layers and equal weights.

The generators are G^{1}and G^2, the discriminators are D^1 and D^2, and is a set of noise that was used encode the real message. The discriminators D^1 and D^2 determine the outcomes based on the AME and FHE conditions, accordingly. They were trained via maximizing the loss based on each determination outcome, as illustrated in Eqs. (4) and (5) utilizing D^1 and D^2 loss correspondingly.

Let,

$$\begin{aligned} \mathrm{Loss\ D1\ (D1, G1)} \\ &= \mathrm{E}_\alpha[\log\ \mathrm{D1}\ (\alpha)] + E_\alpha[1 \\ &- \log \mathrm{D1}\ (\mathrm{G1}\ (\alpha))] \end{aligned}$$

$$\mathrm{Loss\ D2\ (D2, G2)} = \mathrm{E}_\alpha[\log \mathrm{D2}\ (\alpha)] + E_\alpha[1 - \log \mathrm{D2}\ (\mathrm{G2}\ (\alpha))] \tag{4}$$

The generators are trained as shown in Algorithm 1 by optimizing the losses using Loss G^1 (), G^2 (), and (Eq. (3)) by comprehensively considering the determination results of the two discriminators.

$$\mathrm{Loss\ (G1, G2, D1, D2)} = \frac{\mathrm{E}_\alpha\left[1-\mathrm{LOG}\left(\mathrm{G}^1(\alpha)\right)\right]+\mathrm{E}_\alpha\left[1-\mathrm{LOG}\left(\mathrm{G}^2(\alpha)\right)\right]}{2} \tag{5}$$

3.7 Improved CGAN model training algorithm

```
        FUNCTION Back Propagation (α)
        BEGIN
Initialize generator G¹, generator G², discriminator D¹, discriminator D²
        Initialize α
        FOR i←1 to SIZE (number of iterations)
        FOR j←1 to SIZE (number of batch size)
        α update D¹ by Loss D¹ (D¹, G¹)
        Update D² by Loss D² (D², G²)
        Update G¹ by Loss G¹ (D¹, D², G¹)
        Update G² by Loss G² (D¹, D², G²)
        END FOR
        END FOR
        END
```

3.8 Encryption and decryption modules

The fake samples generated by generators and real samples are encrypted and passed through IoT network. Then, the received encrypted text on receiver side are decrypted for further processes. This is illustrated in Figure 2.

3.9 Algebraic Matrix Encryption

A=1	B=2	C=3	D=4	X=-12
E=5	F=6	G=7	H=8	Z=-13
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	

Let the key be $1K_1$,$2K_2$,....K_N where N is the number of words in the message. Also, consider the messages are $1K_5$ =HELLO, $2K_5$ = WORLD. $1K_5$= HELLO can be denoted as: H= 8, E= 5, L= 12, L= 12, O= -2. $2K_5$= WORLD: W= -10, O= -2, R=-5, L=12, D=4 Construct the Cyclic Square Matrix with characters in $K_i$for each i =1, 2,... n, not clear.

$1K_5$

8	5	12	12	-2
5	12	12	-2	8
12	12	-2	8	5
12	-2	8	5	12
-2	8	5	12	12

$2K_5$

-10	-2	-5	12	4
-2	-5	12	4	-10
-5	12	4	-10	-2
12	4	-10	-2	-5
4	-10	-2	-5	12

Now, calculating the E (η ($1K_5$)) and E (η ($2K_5$)) using the following condition.

1. $W_i = \frac{j+1}{2}$ if η $(K_i) =$ j is odd, k $=$ 1, 2 …. n & $and\ I, j =$ 1, 2 ...
2. $W_i = \frac{j}{2}$ if η $(K_i) =$ j is even, k $=$ 1, 2 …. n & $and\ I, j =$ 1, 2 ...

- Then for $1K_5$: η ($1K_5$) = 5, this is an odd number, so using the condition is $\frac{j+1}{2}$ if η $(K_i) =$ j the resultant value is 3. This is similar to η ($2K_5$). Assign each column value as b_1= 12 12 -2 8 5 and b_2= -5 12 4 -10 -2.

where, b_1 and b_2 are the diagonal matrix, respectively.

- Compute the diagonal matrix D (b_1) $-5\mathrm{I}_5$ =D (12 12 -2 8 5)$-5\mathrm{I}_5$ = 7 7-7-3 0 and D (b_2) $-5\mathrm{I}_5$= D (-5 12 4 -10 -2) $-5\mathrm{I}_5$ = -10 7 -1 -15 -7. Hence the encrypted results are M1= 7 7-7-3 0 and M2= -10 7 -1 -15 -7. This encrypted message is forwarded to the FHE encryption module for next stage of encryption.

3.10 Fully Homomorphic Encryption (FHE)

FHE is an encryption technology that performs addition and multiplication at the same time and can compute any operation [2]. Many encryption algorithms have been used to convert plain text to ciphertext and vice versa. However, it is still inefficient and it is not easy to convert text or data because it contains complex mathematical formulas that take longer to process.

3.11 FHE key generation

Let's consider the encrypted results from AME M1 and M2 key sizes like $1K_5\ and\ 2K_5$ = n. Select another number using Eq. (4).

$$\mathrm{S}_1 = \mathrm{n} * u \qquad (6)$$

Next, select one big random integer with the condition, i.e.(R $\leq$ 1 and R $\geq$ 9), therefore

$$\mathrm{e} = \mathrm{R}\ (\mathrm{n} - \mathrm{m} + 1) \qquad (7)$$

Now, the public key is (S_1, e) and the secret key is (n).

3.12 FHE encryption

According to FHE, M1= 7 7-7-3 0 and M2= -10 7 -1 -15 -7 are the messages from IoT. Now, they were utilizing the Eq. (6) to encrypt the message again.

$$\mathrm{C1\ C2} = \mathrm{M1M2}^{\mathrm{ij*e+1}} \mathrm{mod\ S}_1 \qquad (8)$$

where, C1 and C2 are the ciphertexts of message HELLO WORLD, i and j are the two random integers.

Next, the double encrypted message is transmitted to the receiver through the IoT network.

3.13 FHE decryption

The received encrypted IoT data are decrypted in two stages. First, it is decrypted using FHE decryption technique. Then, it is decrypted using FHE decryption technique.

According to FHE, decrypting the ciphertext using Eq. (7).

$$P1P2 = C1C2\ mod\ n \qquad (9)$$

where, P1= 7 7-7-3 0 and P2= -10 7 -1 -15 -7 are decrypted message, n is the secret key.

FHE is used for encrypting the actual message in the other approach of proposed work (hello world). In the first stage, the collected number of character counts in encrypted message is referred to as key size and that message will be considered as P1 and P2.

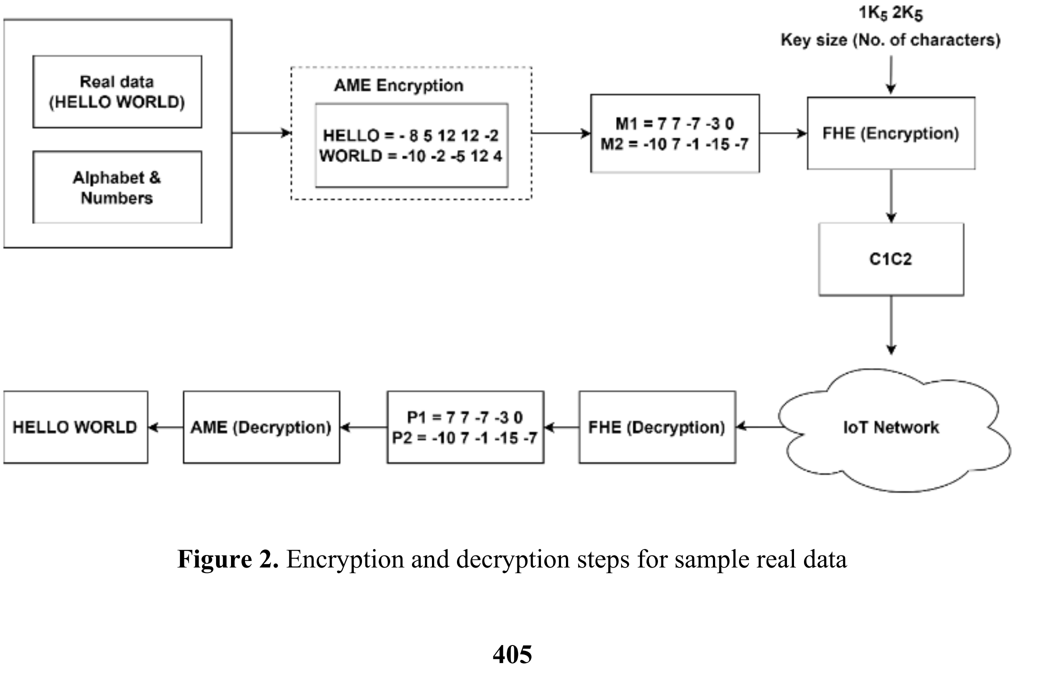


Figure 2. Encryption and decryption steps for sample real data

Algebraic Matrix Decryption

Now, decrypting the $1K_5$ and $2K_5$ with the help of a diagonal matrix. c_1= D (b_1) + $5I_5$ = 17 17 3 13 10 and c_2 = D (b_2) + $5I_5$ = 0 17 9 -5 3. Hence the decrypted results are 17 17 3 13 10 and 0 17 9 -5 3. Now rearrange the values from 1st to 5th, 8 5 12 12 -2, which is HELLO. c_2 = -5 12 4 -10 -2 →3rd 4th 5th 1st 2nd. Now rearrange the values from 1st to 5th, which is WORLD. Finally, this output from the decryption module is send to the discriminator1 for further checking diverse samples.

In this work, Improved FHE encrypts the data (message) to ensure that the message is transferred quickly and securely. When compared to traditional FHE, the improved FHE has lower time complexity. Because the key size in improved FHE is (input) is extracted directly from the IoT message, and no random integer values are used as input at the start.

3.14 Calculation of degree of similarity using Jaro-Winkler similarity

The performance of the generators can be evaluated by checking whether generated fake data are diverse in nature. This is achieved by calculating the degree of similarity between generated fake data. For this, Jaro-Winkler similarity method is adopted. The Jaro-Winkler similarity seems to be a string metric that compares the edit distance of two strings. Jaro Similarity is quite similar to Jaro Similarity. Jarrow compares the similarity of two strings. The Jaro distance has a value between 0 and 1. Where 1 indicates that the strings are equivalent and 0 indicates that the two strings are not similar. The closer the string value is, the greater the distance between the two strings. Whenever the prefixes of two strings match, Jaro-Winkler analogy uses the "p" prefix scale to provide a more accurate result when strings share a common prefix up to a maximum length of l. So, this work considers Jaro-Winkler similarity to find the similarity between generated fake images. When the degree of similarity value was low, it is apparent that the generators' fake samples were diverse in their nature. Hence, the mode collapse problem is resolved.

The Jaro-Winkler similarity can be calculated using following steps:

Step1: Compute the match range (MR) of comparing strings str1 and str2.

$$MR = \frac{\max(len(str1)),(len(str2))}{2} - 1 \qquad (10)$$

Step 2: The Jaro Similarity (Js) can be determined with the help of Eq. (11),

$$Js = \frac{1}{3} * \frac{mc}{|str1|} + \frac{mc}{|str2|} + \frac{mc-t}{mc} \;, mc! = 0 \qquad (11)$$

where, mc denotes the number of matching characters, t denotes half the number of transpositions, $|str1|$ and $|str2|$ denotes the lengths of strings str1 and str2 correspondingly.

The characters were considered to match when they are identical and they are not more than

$$\left\lceil \frac{\max(|str1|,|str2|)}{2} \right\rceil - 1$$

The conversions are half the number of matching characters in both strings, but in a different order.

Step 3: Compute the Jaro Winkler similarity using following formula,

$$Jws = Js + \frac{S}{10} * L * (1 - Js) \qquad (12)$$

where, Jws denotes Jaro-Winkler similarity; S and L denotes the scaling factor and length of the matching prefix up to a maximum of 4 characters.

Algorithm for Jaro-Winkler similarity

```
Input: Two strings str1 and str2
Compute Jaro Similarity of two strings
        if(str1 and str2 are equal)
         return 1;
Calculate length of two strings
$|str1|$ = len(str1) and $|str2|$ =len(str2)
Determine the maximum distance at which matching is permitted.
        $\left\lceil \frac{\max(|str1|,|str2|)}{2} \right\rceil - 1$
    Count number of matches mc and hashes for each string, h_str1 and h_s1
Check to see whether there are any matches in the first string.
        for($i \le |str1|$)
for j in range(max (0, i - max_dist), min ($|str2|$, i + max_dist + 1))
        if (str1[i] == str2[j] and h_str2[j] == 0)
          h_str1[i] = 1;
          hash_str2[j] = 1;
          mc += 1;
          break;
else
 return 0;
end for
    Check Number of transpositions
Determine the number of times two characters match while there is a third matching character between the indices.
return the Jaro Similarity $Js$
    end for
Calculate Jaro-Winkler similarity $Jws$ using step 3.
```

4. WHALE OPTIMIZATION ALGORITHM

The main issue with training the GAN is that it could encounter constraints like mode collapse, vanishing gradients, as well as instability, each of which is influenced by the GAN's hyperparameters. The selection of appropriate hyperparameters is a critical issue which might affect the GAN's output. In this work, the Whale Optimization Algorithm (WOA) is used to optimize the hyperparameters of the GAN.

5. RESULT AND DISCUSSION

Using the following parameters, this section conducted an efficient comparison between the proposed work and the state of the artwork. The parameters are Jaro-Winkler accuracy Test, Training time, Loss of Generator and Discriminator, Root means square error (RMSE), mean absolute error (MAE), percent root mean square difference (PRD), recall, F-score, mean and standard deviation. This study uses two current approaches to assess the performance of the proposed work as MTC-GAN [5].

Table 1. Training parameters

Parameters	Value
Number of iterations for Optimization	20
Activation function	Sigmoid
Number of search agents	20
Validation frequency	1000
Training algorithm	Adam
Batch size	64
Adam number of epochs	150

Table 2. Measurement of Jaro-Winkler accuracy similarity

S.No.	String 1	String 2	Measurement of Similarity	Conclusion
11	Tagang	Dagang	0.92	No mode collapse
22	Find	Fine	0.93	No mode collapse
33	Mape	Mape	0	Mode collapse
44	Take	keta	0.83	No mode collapse
55	Lose	Loss	0.87	No mode collapse

The WOA is used in hyperparameter optimization because it keeps the transition between exploration and exploitation as seamless as possible. Table 1 shows the optimal hyperparameters determined using the WOA. The activation function used here is the sigmoid function. If a neuron's activation function seems to be a sigmoid function, then the output of this neuron will be typically between 0 and 1.

The Jaro-Winkler algorithm and GSO-COFC is to determine the accuracy of the model. Table 2 denotes the five sample values for two strings, string 1 and string 2 and it depicts that the similarity value for two strings using Jaro-Winkler algorithm and GSO-COFC. The similarity value for third sample is 0, which indicates both strings are same and final conclusion is there occurs a mode collapse problem.

The difference between actual and generated data is measured by the RMSE value and is defined as:

$$RMSE = \sqrt{n \sum_{i=1}^{n} (R_i - F_i)^2} \tag{13}$$

The average absolute error between the generated and the real data is calculated using the term "mean absolute error" and it can be defined as:

$$MAE = \frac{1}{n} \sum_{i=1}^{n} |R_i - F_i| \tag{14}$$

By using the percent root mean square difference, the distortion between the real and generated data can be calculated which is shown in below equation.

$$PRD = \sqrt{100 \frac{\sum_{i=1}^{n} (R_i - F_i)^2}{\sum_{i=1}^{n} (R_i)^2}} \tag{15}$$

Table 3 shows the performance comparison for proposed model and existing techniques. While comparing proposed model in terms of RMSE, MAE, PRD, recall and F-score, the proposed model indicates better results than MTC-GAN and AEGAN models. It is because the dual generator generates fake data samples and if not, the discriminators send feedback to generators to avoid mode collapse problem.

Table 3. Performance comparison for proposed model

Parameters	Methods		
	MTC-GAN	AEGAN	Proposed Method
RMSE	0.57	0.49	0.45
MAE	0.54	0.51	0.48
PRD	62.2	56.8	51.1
Recall	60.35	68.18	71.25
F-score	80.65	85.23	87.12

Figure 3 shows the loss variance in the proposed model, and due to the large losses from epoch 1 to 7, the model was pre-trained to deal with them to reduce the loss to a certain level. Table 4 shows the performance of various methods in terms of loss and training time.

Table 4. Results of the proposed model with existing techniques

Parameters	Proposed Model	[18]	[19]
Epoch	150	150	150
Training Time	42min	45min	270min
Loss of Generator	2.5678	2.699	15.714
Loss of Discriminator	1.480	1.570	4.617

Encryption time:

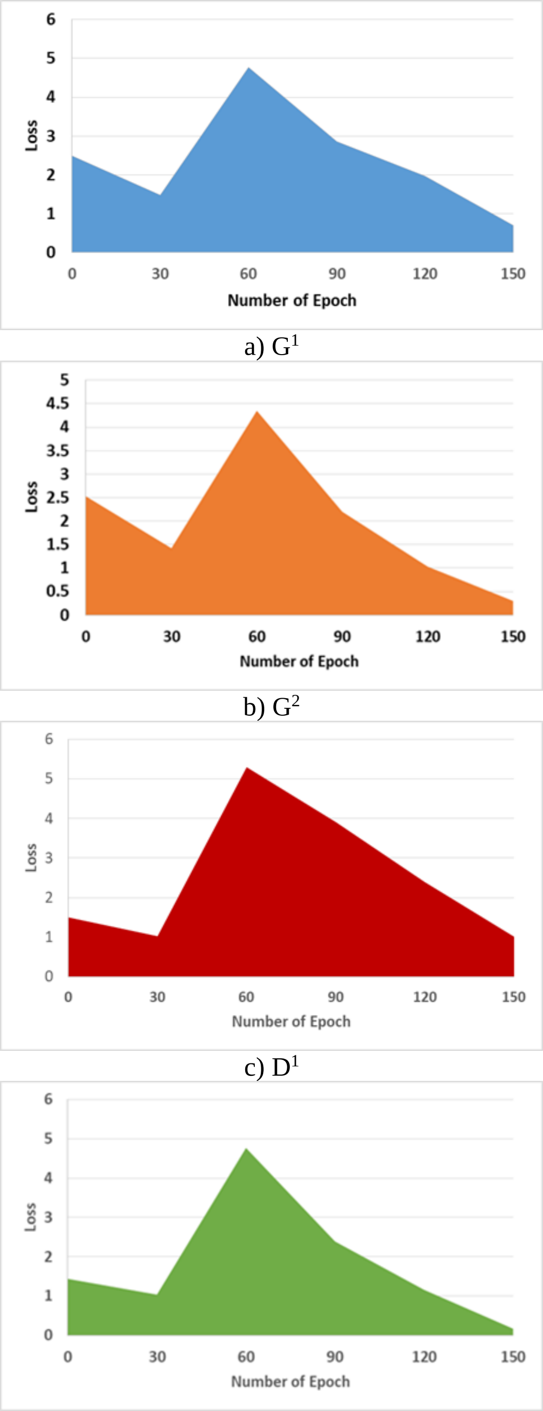
The proposed algorithm is shown in Table 5 and in comparison of the AEGAN and MTC-GAN algorithms. The proposed approach works best for messages of various sizes from 200 KB to 450 KB. Improved CGAN can be applied to larger amounts of data and with less encoding time.

Table 5. Encryption time

Data Size in kb	MTC-GAN	AEGAN	Proposed Method
200	1.2	1.1	0.0598
250	1.7	1.3	0.066
300	2.4	1.6	0.072
350	3.6	2.4	0.0791
400	4.2	2.6	0.0876
450	4.7	3.2	0.0953

The generating loss G1, as demonstrated in Figure 3 (a), began at Epoch 0 at 2.490, suddenly increased to 1.480 at Epoch 30 because of the discriminator processing the encryption operation, and finished at epoch 150, with the loss of 0.7. Also, the generating loss G2, as demonstrated in Figure 3 (b), began at Epoch 0 at 2.527 and finished at Epoch 30 at 1.423. At Epoch 150, the loss is 0.3. The MTC-GAN loss variation is shown in Figure 4, and AEGAN loss variation is shown in Figure 5.

When compared to existing works, the generator of the proposed work achieves a loss value of 2.5678, which is 13.14% lower than MTC-GAN and 0.1312% lower than AEGAN. Similarly, the loss of discriminator for the proposed work is 1.480, which is 3.137% lower than MTC-GAN and 0.09% lower than AEGAN. This low value indicates the effectiveness of the proposed work.



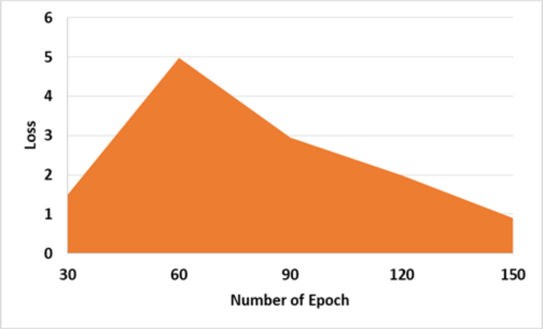
a) G[1]

b) G[2]

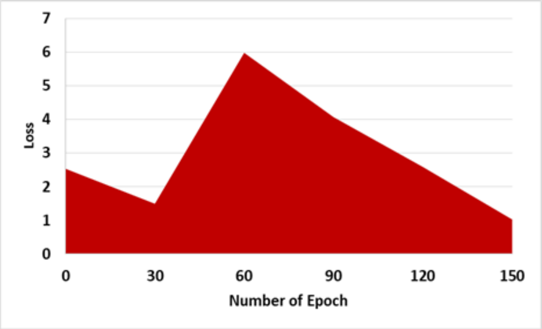
c) D[1]

d) D[2]

Figure 3. Results of the proposed work



a) Loss of generator



b) Loss of discriminator

Figure 4. Results of MTC-GAN from Zhang et al. [18]

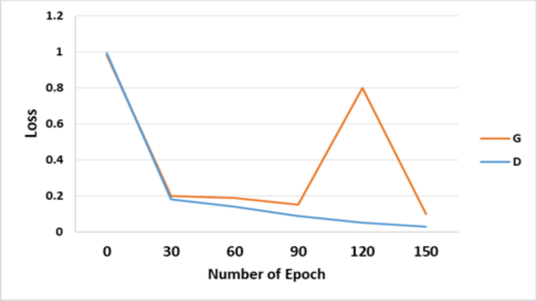


Figure 5. Results of the AEGAN from Wu et al. [23]

Also, the GAN hyperparameters tuned using WOA enhances the performance of the proposed work, thereby decreasing the loss value which is comparatively lower than the other methods. This further reduces the overfitting and instability problems in the proposed method. Additionally, it eliminates the problem of mode collapse in CGAN. The humpback whale's special hunting trick is used in WOA to find the best search agent for the generator in the given space.

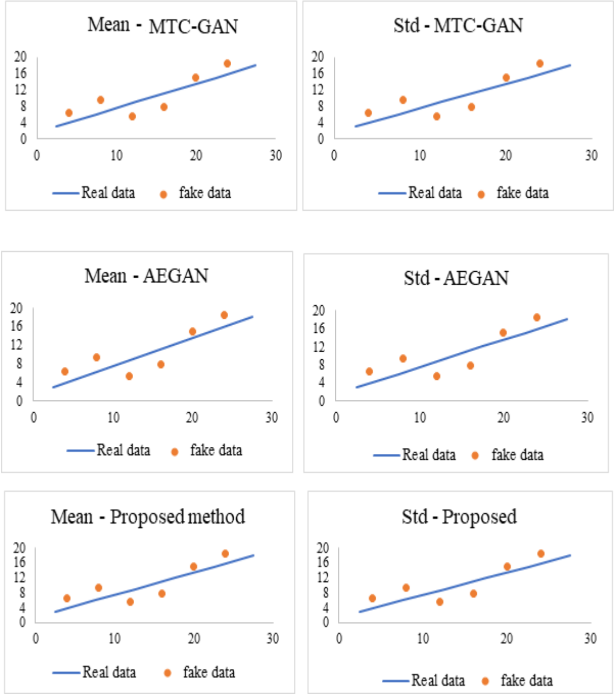


Figure 6. Results of mean and standard deviation for different GAN models

Another useful method for assessing the similarity between real and fake data visually is the estimation of mean and standard deviation. The plotted points in Figure 6 are the generated data, whereas the blue line in the Figure 6 reflects the original data. The similarity between the real and fake data is higher the closer the spots are to the blue line. The mean and standard deviation of real and fake data produced by AEGAN, MTC-GAN, and the proposed approach have been compared. Results demonstrate that the proposed model performs more effectively than other GAN models since the generated data is close to the diagonal.

6. DISCUSSION

Conditional Generative Adversarial Network (CGAN) is one of deep learning techniques that protects data based on conditions generated by constructor and identifier models. CGAN helps to retrieve selected features from generated data. This task exploits the potential of CGAN to control the data encryption and decryption part of the GAN network. In GANs, attackers can exploit corrupted nodes to inject erroneous data, compromising the integrity of network data. To address the shortcomings of private isomorphic encryption, we focus on achievable FHE for end-to-end data privacy in CGANs.

The designed FHE can be implemented in sensor nodes, where the assembler can perform infinite computational ciphertext assembly functions. In order to detect false data early in the process of data transmission and aggregation, we propose a CGAN network structure consisting of monitoring nodes, forwarding nodes, and aggregator adjacent nodes. In this configuration, forwarding nodes and neighboring nodes verify data computed by the same set of observer nodes and detect spurious data as soon as it appears. Therefore, this structure reduces the data transmission in the network with damaged nodes. The advantage of using an algebraic matrix is that it can reduce the time complexity and input complexity in the encryption process. Addition and multiplication can be performed simultaneously, and all operations can be calculated immediately. Therefore, in this work, we consider solving the time complexity problem by solving the simplest mathematical derivation of the decoding part. In addition, we found that the homomorphic encryption algorithm has a shorter encryption time.

7. CONCLUSION

IoT is being deployed and harnessed globally to address some of the most pressing issues in global development. This phenomenon brought various issues, including reliability, safety, and enhancement in a range of fields, due to significant advances in wireless and mobile communication technology. The risks associated with IoT security, notably the fundamental issue of data confidentiality and integrity while data is being transported from IoT devices to servers through the internet, can be properly mitigated and handled with propriety. This paper proposed a deep learning-based CGAN model to guarantee safe data transmission. To improve the operation of CGAN, two generators and two discriminators were deployed, and the mode collapse problem was solved in this work. In addition, the two proposed encryption algorithms are employed to send the messages safely to the receiver. To find whether generated fake samples are diverse in nature. According to experimental data, the proposed method outperforms others in terms of Jaro-Winkler accuracy test, training time, loss, Root means square error (RMSE), mean absolute error (MAE), percent root means square difference (PRD), recall, F-score, mean, and standard deviation. The proposed model's generator loss was about 82.8%, that was less than the loss of the generator in the standard models. By using mean and standard deviation, similarity between real and fake data are visualized.

The proposed model's discriminator loss was about 66.0 percent, which is lower than the traditional model's (4.617). This could be used in other fields in the future, such as disease diagnosis, where the mode collapse problem can be solved and high-accuracy disease diagnosis is possible. Also, we planned to reduce encryption cost in future.

AUTHORS' CONTRIBUTION

A.P.G contributed to technical and conceptual content, architectural design. R.S contributed to guidance and M.V counseling on the writing of the paper.

REFERENCES

[1] Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I., Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3): 1646-1685. https://doi.org/10.1109/COMST.2020.2988293

[2] Purswani, J., Rajagopal, R., Khandelwal, R., Singh, A. (2020). Chaos theory on generative adversarial networks for encryption and decryption of data. In: Jain, L., Virvou, M., Piuri, V., Balas, V. (eds) Advances in Bioinformatics, Multimedia, and Electronics Circuits and Signals. Advances in Intelligent Systems and Computing, vol 1064. Springer, Singapore. https://doi.org/10.1007/978-981-15-0339-9_20

[3] Shaikh, F., Ghani, N., Bou-Harb, E. (2019). IoT Threat Detection Leveraging Network Statistics and GAN. University of South Florida, Technical Report, 9.

[4] Zhang, X., Zhang, S., Lin, J., Sun, F., Zhu, X., Yang, Y., Tong, X., Yang, H. (2019). An efficient seismic data acquisition based on compressed sensing architecture with generative adversarial networks. IEEE Access, 7: 105948-105961. https://doi.org/10.1109/ACCESS.2019.2932476

[5] Huang, J., Le, Z., Ma, Y., Fan, F., Zhang, H., Yang, L. (2020). MGMDcGAN: Medical image fusion using multi-generator multi-discriminator conditional generative adversarial network. IEEE Access, 8: 55145-55157. https://doi.org/10.1109/ACCESS.2020.2982016

[6] Nguyen, T., Le, T., Vu, H., Phung, D. (2017). Dual discriminator generative adversarial nets. Advances in Neural Information Processing Systems, 30.

[7] Li, S., Jang, S., Sung, Y. (2019). Automatic melody composition using enhanced GAN. Mathematics, 7(10): 883. https://doi.org/10.3390/math7100883

[8] Shihab Hamad, S., Sagheer, M.S. (2018). Public key fully homomorphic encryption. Journal of Theoretical and Applied Information Technology, 96.

[9] Wu, D.N., Gan, Q.Q., Wang, X.M. (2018). Verifiable

public key encryption with keyword search based on homomorphic encryption in multi-user setting. IEEE Access, 6: 42445-42453. https://doi.org/10.1109/ACCESS.2018.2861424

[10] Wang, X., Luo, T., Li, J. (2018). A more efficient fully homomorphic encryption scheme based on GSW and DM schemes. Security and Communication Networks, 2018: 1-14. https://doi.org/10.1155/2018/8706940

[11] Bhatia, D., Dave, M. (2019). Partial and fully homomorphic encryption schemes for privacy preserving. In Proceedings of International Conference on Advancements in Computing & Management (ICACM). http://doi.org/10.2139/ssrn.3446667

[12] Tang, H., Xu, D., Wang, W., Yan, Y., Sebe, N. (2019). Dual generator generative adversarial networks for multi-domain image-to-image translation. arXiv preprint arXiv:1901.04604. https://doi.org/10.48550/arXiv.1901.04604

[13] Cho, J., Yoon, K. (2020). Conditional activation GAN: Improved auxiliary classifier GAN. IEEE Access, 8: 216729-216740. https://doi.org/10.1109/ACCESS.2020.3041480

[14] Wu, D., Cao, H., Li, D., Yang, S. (2020). Energy-efficient reconstruction method for transmission lines galloping with conditional generative adversarial network. IEEE Access, 8: 17310-17319. https://doi.org/10.1109/ACCESS.2020.2966739

[15] Yu, Y., Srivastava, A., Canales, S. (2021). Conditional LSTM-GAN for melody generation from lyrics. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 17(1): 1-20. https://doi.org/10.1145/3424116

[16] Palanisamy, I., Santha, T. (2021). Machine learning based secured data transmission for banking application. Annals of the Romanian Society for Cell Biology, 5225-5237.

[17] Mohammadjafari, S., Cevik, M., Basar, A. (2023). VARGAN: Variance enforcing network enhanced GAN. Applied Intelligence, 53(1): 69-95. https://doi.org/10.1007/s10489-022-03199-8

[18] Zhang, M., Li, C., Zhou, Z. (2021). Text to image synthesis using multi-generator text conditioned generative adversarial networks. Multimedia Tools and Applications, 80: 7789-7803. https://doi.org/10.1007/s11042-020-09965-5

[19] Liu, B., Wang, L., Wang, J., Zhang, J. (2023). Dual discriminator weighted mixture generative adversarial network for image generation. Journal of Ambient Intelligence and Humanized Computing, 14(8): 10013-10025. https://doi.org/10.1007/s12652-021-03667-y

[20] Wang, L., Sun, Y., Wang, Z. (2022). CCS-GAN: A semi-supervised generative adversarial network for image classification. The Visual Computer, 38: 2009-2021. https://doi.org/10.1007/s00371-021-02262-8

[21] Li, K., Peng, S., Zhang, T., Malik, J. (2020). Multimodal image synthesis with conditional implicit maximum likelihood estimation. International Journal of Computer Vision, 128: 2607-2628. https://doi.org/10.1007/s11263-020-01325-y

[22] Bharti, V., Biswas, B., Shukla, K.K. (2022). EMOCGAN: A novel evolutionary multiobjective cyclic generative adversarial network and its application to unpaired image translation. Neural Computing and Applications, 34(24): 21433-21447. https://doi.org/10.1007/s00521-021-05975-y

[23] Wu, Z., He, C., Yang, L., Kuang, F. (2021). Attentive evolutionary generative adversarial network. Applied Intelligence, 51: 1747-1761. https://doi.org/10.1007/s10489-020-01917-8

[24] Yang, H., Lu, X., Wang, S.H., Lu, Z., Yao, J., Jiang, Y., Qian, P. (2021). Synthesizing multi-contrast MR images via novel 3D conditional Variational auto-encoding GAN. Mobile Networks and Applications, 26: 415-424.