Journal of Information Systems Engineering and Management
2025, 10(18s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security Enhancement and Attack Detection using Humboldt Squid Optimized Extended Paillier AES Encryption Scheme and Guided Attentional GAN over Internet of Things

Sanjay Kumar[1*], Dr. C.S.pillai[2]
[1*]*Assistant professor, Department of CSE(AI&ML), Don Bosco Institute of Technology,Kumbalgodu, Mysore Road,Bengaluru-560074*
[2]*professor, Department of CSE(Data Science), ACS College of Engineering, Kambipura, Mysore Road, Bengaluru-560074*
[1*]*Corresponding Author Email: sanjaykumar@dbit.co.in*

ARTICLE INFO

Received: 16 Dec 2024

Revised: 25 Jan 2025

Accepted: 10 Feb 2025

ABSTRACT

The Internet of Things (IoT) has seen an increase in applications due to the exponential growth of smart devices and the decline in sensor costs. Although Internet traffic tracking and categorization have been thoroughly examined over the last 10 years, this is still popular in the IoT space. This manuscript proposes a novel attack detection framework and improved encryption scheme for secure data transmission in IoT networks. Initially, the raw data samples collected from the NSL-KDD dataset are preprocessed by performing a normalization process using a variable stability scaling technique. Then, the guided attentional generative adversarial network (GAtt-GAN) technique is proposed to detect and classify the various malware attacks like U2R, DoS, R2L, Probing, normal, and unknown accurately. In addition to this, the Extended Paillier-boosted Advanced Encryption Standard (ExP-AES) technique is introduced in this framework. By taking advantage of this characteristic, the AES-encrypted keys are optimally selected using the Humboldt Squid Optimizer (HBSO) technique, preserving the transmitted data's validity and confidentiality. The method makes use of an adaptive key turnover mechanism that makes the encryption process more unpredictable and fortifies its resistance to cryptographic attacks. Various performance measures areanalyzed, like encryption time, decryption time, throughput, accuracy, F-measure, false discovery rate (FDR), reliability, security level analysis, encryption, and decryption time, and compared with the proposed framework to prove the model's efficacy. The overall accuracy of 98.5%, F-measure of 98.07%, and FDR of 0.042, as well as encryption and decryption time of 117.5s, are obtained by the proposed framework for providing security against IoT vulnerabilities.

Keywords: Internet of Things, Secure Data Transmission, Attack Classification, Deep Learning (DL), Cryptographic Mechanism, Encryption, Data Normalization, Optimal Key Selection.

INTRODUCTION

Over the past few decades, the number of interconnections to multiple things in various sectors, including business, homes, and transportation, has rapidly expanded due to the widespread use of the Internet of Things (IoT) [1, 2]. IoT-capable gadgets come in the smallest sizes and measure the temperature using home appliances using microcontrollers, such as air conditioners, ovens, flat screens, and large producing apparatus [3]. These devices transmit data and communicate via the internet with the cloud server for examination. Taking into account that security is crucial, Signals used in wireless communications are broadcast in nature and are sent through channels accessible to unapproved gadgets or nodes [4, 5]. Due to the IoT's' reliance on wireless connectivity and the growing number of devices that are being added to the network, safeguarding devices on the IoT platform is increasingly vital. In [6], the device with the least security is the most vulnerable to cyberattacks, which can steal the majority of personal data that is already on connected devices on the internet [7, 8]. Due to the constant rise in the number of devices linked in the network and the volume of data these devices collectively generate, security is the main IoT concern. Numerous studies on IoT networks have indicated that confidentiality and safety of data are the two most crucial factors to take into account while using this system of connected equipment [9, 10].

Furthermore, the attacker can able to access the distributed network using devices that have a weak point of security against invading devices [11]. Consequently, a range of classification techniques, including LSTM, RNN, DNN, DBM, and RBFN, are employed to identify malware or assaults in Internet of Things networks. Additionally, file communication between devices in an IoT network requires secure data transmission [12, 13]. The quantity of keys used in the cryptographic process determines the data's level of protection. There are cryptography techniques that are used to guarantee privacy, like blowfish, DES, and ECC. Moreover, the two primary groups of cryptographic techniques are symmetric and asymmetric cryptography [14, 15]. Symmetric key cryptography (SKC) uses a shared secret key among all participants in the community, while asymmetric key cryptography (AKC) protects data by using dual keys [16, 17]. AKC in WSN requires a longer computational period for data encryption and decryption, while SKC necessitates greater capacity for maintaining the key among all connected nodes [18, 19]. These specific security challenges are brought about by the scarce resources of edge devices paired with IoT communications protocols [20].

Motivation: The rapid proliferation of IoT devices transformed a variety of sectors, from smart homes to healthcare and industrial applications. This unprecedented growth brought about very serious security challenges. According to a report by cybersecurity firms, IoT devices are increasingly becoming targets for cyberattacks due to their usually limited security features. This growing vulnerability raises the need for robust mechanisms for security in the protection of data integrity and privacy in IoT environments. Many IoT devices have constrained processing power and memories that impede the implementation of complex security protocols. Traditional methods of encryption that require huge computational resources are rendered impracticable on most of these devices, leaving them more susceptible to unauthorized access. Cyberattack techniques continuously evolve, making static defenses ineffective over time. Furthermore, IoT devices generate a huge volume of data, which floods traditional network security systems and makes threat identification and mitigation difficult in real time. Also, many of the deployed security measures do not handle the continuous monitoring requirements of an IoT network or the delivery of anomaly detection capabilities that allow any system to quickly identify and respond to unusual behavior, leaving it open to existing and emerging threats alike. Moreover, the integration of deep learning for attack classification makes the detection of threats dynamic. Deep learning (DL) algorithms can process huge amounts of data generated through IoT devices to identify patterns indicative of attacks, such as DDoS and data exfiltration attempts. These learn from past and real-time data, adapting to new threats that maybe were not classified earlier and improving the security posture.

The main contributions of the proposed framework are encompassed as follows:

- ❖ To introduce a novel attack detection framework and optimal data encryption technique (GAttGAN-HBSO-ExPAES) for enhancing the security of the Internet of Things (IoT).
- ❖ To propose a variable stability scaling (Var-SS) technique for the data normalization process to maintain a high correlation among the data instances.
- ❖ To conquer an innovative guided attentional generative adversarial network (GAtt-GAN) for classifying various attacks like U2R, DoS, R2L, Probing, normal, and unknown with minimal error and low processing time.
- ❖ To present an Extended Paillier-boosted Advanced Encryption Standard (ExP-AES) technique for promoting secure data transmission in IoT systems.
- ❖ To contemplate the Humboldt Squid Optimizer (HBSO) technique for the optimal selection of private and public keys in the Paillier Cryptosystem.
- ❖ To substantiate the effectiveness of the proposed method by scrutinizing various computational measures like encryption time, decryption time, throughput, accuracy, F-measure, false discovery rate (FDR), reliability, security level analysis, encryption, and decryption time, and compared with the proposed framework to prove the model's efficacy.

The upcoming sections are prearranged as follows: Section 2 outlays the related work, Section 3 deliberates over the suggested approaches, Section 4 presents the results and discussion, and the conclusion of the suggested framework is deliberated in Section 5.

RELATED WORKS: A BRIEF REVIEW

Among the several studies on IoT data security, some current research works are discussed in this section:

In 2022, Chen *et al.*, [21] have defined the symmetric cryptographic mechanism for preserving the data in IoTs. Here, a secured traffic tracking system was introduced that was both efficient and confidential. To ensure both security and confidentiality inside each inspection round, the technique solely makes use of modest cryptographic operations. Potential disagreements between the clients and servers were also intended to be resolved through an arbitration process. Additionally, the relevant security proof and experimental assessment were provided, which show that the utilized technique performs well and achieves excellent anonymity and security retention. However, the encryption time was high while processing larger data.

In 2022, Das *et al.,* [22] have introduced a combined encryption scheme for medical data security for healthcare IoT systems. To safeguard clinical information in IoT-enabled health services, this scheme provides a encryption mechanism that makes use of ECC, AES, and Serpent. By combining SAEapproaches, the utilized hybrid technique enhances healthcare privacy safeguards. Furthermore, the suggested plan uses an ECC-based numerical signature to satisfy data probity. To further illustrate the efficacy of the recommended strategy for action, the framework included comparisons of efficacy in addition to formal security assessments. The introduced scheme also demonstrated the Findings and analysis to verify the model's efficacy. However, the encryption time was high while processing larger data.

In 2023, Rupa *et al.,* [23] have established an effective security scheme using an improved encryption scheme. Here, a Martino homomorphic encryption (MHE) method based on matrix conversions was put forth, which involved shifting, rotating, and transposing every element in the normal text's ASCII values after they were transformed to binary. Symmetric cryptography uses an identical private key for both encoding and decoding. A desired aspect of symmetric encryption was the "avalanche effect," which occurs when two different keys produce different codes for identical communication. This strategy helps to produce this effect because the key has distinct criteria. This algorithm's linguistics reveals that it was more resilient than the existing encryption method to various forms of attack, so that a statistical analysis by an adversary cannot simply determine the plaintext. However, MHE relies heavily on the use of random numbers for key generation. Poor random number generation can lead to predictable keys, compromising security.

In 2021, Abroshan, *et al.,* [24] have presented a combined encryption scheme for enhancing cloud security using asymmetric and symmetric schemes. Here, suggested a low-impact, highly efficient cryptographic technique to boost cloud computing (CC) security. In CC, dispensation speed was crucial, therefore anintricate cryptographic mechanism was deliberated. Consequently, this approach combines an ECCwith an optimal version of the Blowfish (BF) algorithm. Performance and security were improved by using the ECC algorithm to encrypt the key and BF to encrypt the data. To further guarantee data integrity, a digital signature approach was applied. Throughput, execution time, and memory consumption metrics all improved once the solution was assessed. However, the complexity of this encryption also means that fewer developers may be familiar with its intricacies compared to more widely used systems, leading to potential misconfigurations and inadequate security practices.

In 2023, Jalasri and Lakshmanan [25] have illustrated the data security scheme in IoT fog computing scenarios based on encryption and clustering mechanisms. Here, suggested a low-impact, highly efficient cryptographic technique to boost cloud computing (CC) security. In CC, processing speed was crucial, therefore a complicated cryptographic technique was utilized. Consequently, the approach combines an ECC-based technique with an enhanced version of the Blowfish (BF) algorithm. Performance and security were improved by using the ECC algorithm to encrypt the key and BF to encrypt the data. To further guarantee data integrity, a digital signature approach was applied. Throughput, computation time, and memory utilization metrics all improved once the solution was assessed. However, the scheme was mathematically complex compared to traditional public key cryptosystems. This complexity can lead to implementation errors, which may compromise security.

In 2022, Umapathy and Kalpana [26] have determined the SC method for minimizing the complexity of data security. To secure the CS data, a novel multi-layered cryptographic method known as UK has been introduced here in an attempt to address the need for an alternative solution. To safeguard the data, this UK algorithm employs a completely new transformation process. Even though using violence requires ever greater complexity, it generates enormous complexity in an appropriate period for encoding. To prevent the CS SP from acting in any way within this structure, the crucial information and descriptions were not stored anywhere. In this instance, the information storage SP has possession of the secured information of the client which cannot be accessible by any assaulting techniques. Hence, the CS supplier acquires the distribution center provider. However, the processing power required for these operations can lead to higher energy consumption, which was a vital concern for battery-powered IoT devices that require energy efficiency.

In 2024, Al-Shargabiet *al.,* [27] have introduced the DNA-based SE technique to secure IoT device data. Here, an inflatable DLSE approach based on DNA was intended to be applied to a variety of IoT devices, offering configurable multi-encryption rounds and straightforward operations. To provide a unique key for every round, the DLSE method's private key was generated from an arbitrary arrangement of DNA, making it more challenging for attackers to decode. In comparison to AES and 3DES, the trials demonstrate that the DLSE approach performs exceptionally well, offering the best encoding time and best-distorted percentage at the greatest level of confidentiality. Furthermore, the DLSE approach demonstrated efficiency and was adaptable to the processing capabilities of IoT devices. However, the complex operations required for homomorphic encryption can increase the time it takes to perform computations, leading to higher latency. This can be problematic in real-time IoT applications where timely data processing was critical.

PROPOSED METHODOLOGY

This manuscript proposes a novel attack detection framework and improved encryption scheme for secure data transmission in IoT networks. Initially, the raw data samples collected from the NSL-KDD dataset are preprocessed by performing a normalization process using a variable stability scaling technique. Then, the guided attentional generative adversarial network (GAtt-GAN) technique is proposed to detect and classify the various malware attacks like U2R, DoS, R2L, Probing, normal, and unknown accurately. In addition to this, the Extended Paillier-boosted Advanced Encryption Standard (ExP-AES) technique is introduced in this framework. By taking advantage of this characteristic, the AES-encrypted keys are optimally selected using the Humboldt Squid Optimizer (HBSO) technique, preserving the transmitted data's validity and confidentiality. The method makes use of an adaptive key turnover mechanism that makes the encryption process more unpredictable and fortifies its resistance to cryptographic attacks. Figure 1 depicts the Workflow of the Proposed Method

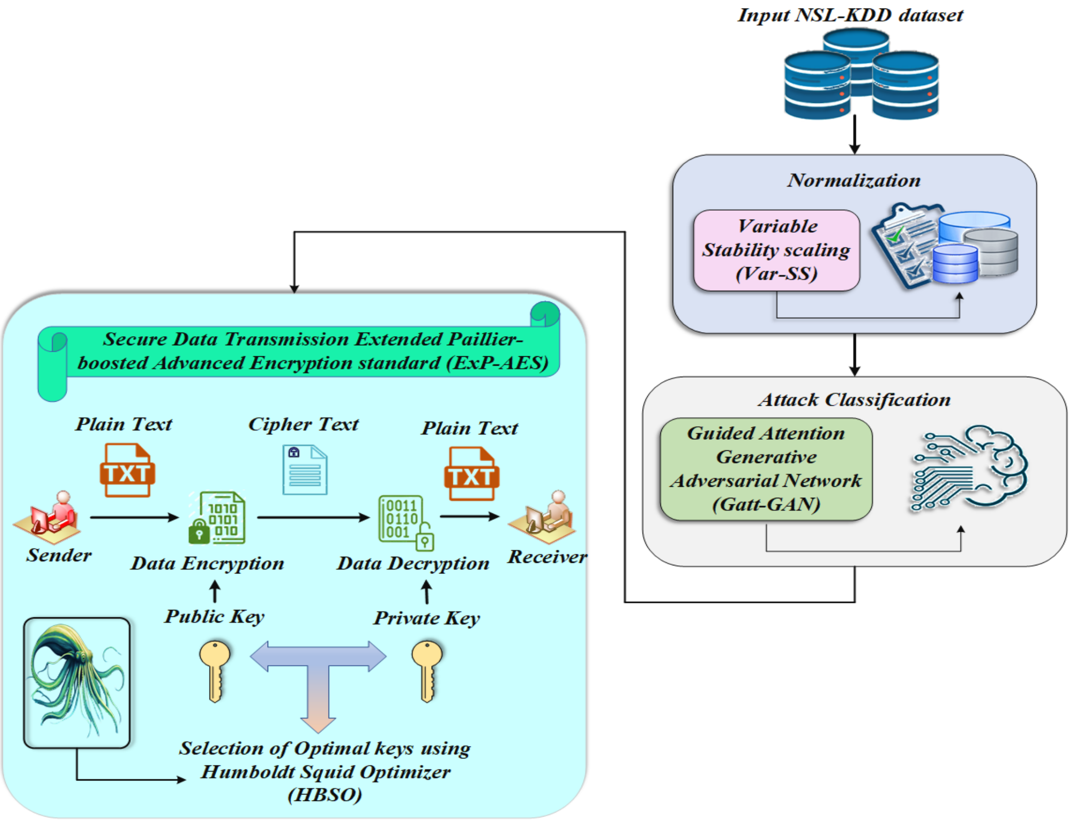
Input NSL-KDD dataset
Normalization
Variable Stability scaling (Var-SS)
Attack Classification
Guided Attention Generative Adversarial Network (Gatt-GAN)
Secure Data Transmission Extended Paillier-boosted Advanced Encryption standard (ExP-AES)
Plain Text
Cipher Text
Plain Text
TXT
TXT
Sender
Data Encryption
Data Decryption
Receiver
Public Key
Private Key
Selection of Optimal keys using Humboldt Squid Optimizer (HBSO)

Figure 1: Workflow of the Proposed Method

Data Acquisition

The NSL-KDD dataset [28] is a widely used benchmark for evaluating network intrusion detection systems (NIDS). It is an improved version of the KDD Cup 1999 dataset, designed to address issues like redundant records and class imbalance, making it more suitable for realistic performance evaluation. The dataset consists of 41 features and a class label, capturing various aspects of network traffic, including basic connection information, content features, and time-based or host-based traffic features. These features help in identifying different types of network intrusions, categorized into four main classes: Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probe attacks, alongside normal traffic. The dataset is divided into training and testing subsets, allowing for robust evaluation of models.

Preprocessing Stage

After Data Acquisition, normalization is performed to maintain a high correlation among the data instances. To perform this, the variable stability scaling (Var-SS) technique is introduced which is the extension of the conventional z-score normalization scheme [29].

In this technique, a variation coefficient is used as a scaling factor which is represented as the ratio of mean data to the standard deviation (SD). It can be mathematically formulated in equation (1),

$$\hat{z}_{a,m} = \frac{\left(Z_{a,m} - \lambda_a\right)}{\sigma_a} \times \frac{\lambda_a}{\sigma_a} \tag{1}$$

Here, λ_a and σ_a indicates the mean and SD of a^{th} feature. The variation coefficient gives greater importance to the samples having less SD and shows lesser importance to the higher SD.

Attack Classification using GAtt-GAN Technique

The preprocessed data are then fed into the GAtt-GAN model to classify multiple attacks like U2R, DoS, R2L, Probing, normal, and unknown accurately. However, the traditional GAN technique [30] is not effective GANs due to increased mode collapse, where itgenerates unrealistic features or fails to encapsulate the full distribution of the training data. The developed architecture contains three major stages: generator, guided attention (GAtt) module, loss function, and discriminator. The advanced generator is comprised of multiple convolutional (Conv) layers that learn the abnormal condition by training large amounts of data. It contains six different phases that learn the relevant features for the classification process. In every stage, Conv layers are introduced that take model input. For extracting the features, LSTM layers are utilized and it is extended up to six times. A stacked network is introduced to enhance the model parameters and balance the classification performance. Moreover, intra-phase iterative unfold residual blocks (RB) are utilized to minimize the network parameters. The detailed analysis of the developed architecture is conquered below:

Generator Module

In this stage, six phases are concatenated comprised of ReLU activation function, Conv-LSTM layers, and RBs. The single RB is iteratively extended five times thereby minimizing network parameters. The strides are 1 with its kernel size of three and a total of 32 filters are considered in ReLU for both input and output. In addition to this, 32 filters are considered in Conv layers present in LSTM and RB layers. As a result, the final Conv layers accept the outcome of RBs with 32 filters and output the generated outcome with a solitary filter.

Discriminator Module

The outcome of the generator is given as input to the discriminator blocks. In the discriminator block, 8 layers are present that provide adversarial outcomes based on the generated outcome. The initial six layers consist of Conv layers and the final two contain the fully connected (FC) layers. For all the layers, the kernel size is set to three, and Conv kernels are 64 for the initial two layers. For the next two layers, the Conv kernels are folded as 128 and the fifth-sixth layer has a total of 256 Conv kernels. Alternately, stride 1 is set for all Conv layers, and the final layer outputs the decision variable for multiclass classification. In the discriminator block, the Leaky ReLU function is utilized as the activation function. Figure 2 illustrates the architecture of the GAttGAN technique.

Guided Attention Module

The regions from different images contain the inheritance and inconsistent distribution of texture, shape, color, variance, illumination, etc. Such inconsistencies are often extracted in three consecutive features X_{k-1}, X_k, and X_{k+1} are fed as input into the three-stream Attention module enabling the network to deliberate into the adaptive learning model. In this module, a single Convolution (Conv) layer and quadruple residual blocks (RBs) are present under each stream, and features are extracted in an increasing order separately under each stream. The features extracted from the Conv layers are fused and given into the RBs to excerpt the depth-level features from the diseased images. Using the Parallel streams, the interaction between the adjacent features can be determined effectively. The in-between features of the nearby streams $Z \in \Re^{w \times h \times c}$ and $Y \in \Re^{w \times h \times c}$ are modified to improve the primary attentive features $\widehat{Z}$ and $\widehat{Y}$ using the soft attentive mechanism. The guided attentive (GAtt) module helps to determine a correlation matrix $P \in \Re^{wh \times wh}$ for generating joint improvements and fusion between two feature subsets. The mathematical expression from the GAtt module is encompassed in equations (2-4):

$$U = \lambda\left(\widehat{Y}^T\right) w \lambda\left(\widehat{Z}\right) \tag{2}$$

$$\widehat{Z}' = \widehat{Z} M_{row}\left(U\right) \tag{3}$$

$$\widehat{Y}' = \widehat{Y} M_{col}\left(U\right) \tag{4}$$

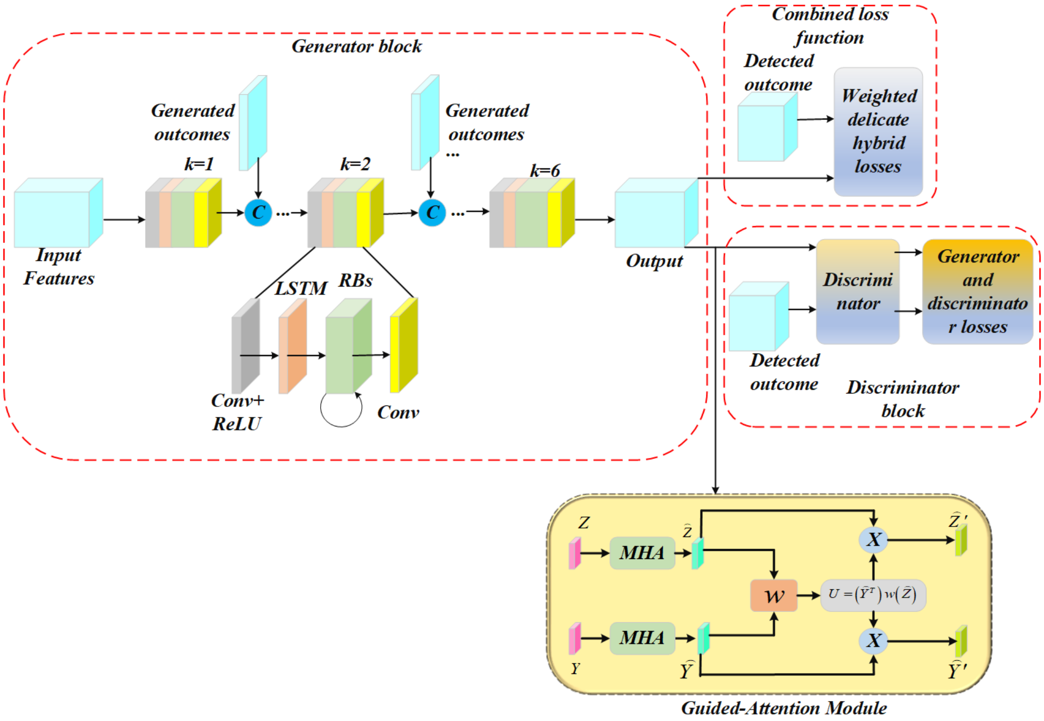

Figure 2: Architecture of the GAttGAN technique

Here, λ indicates the linear transformation that subsets to lower-dimensional features, w indicates the learnable weight matrices, M_{row} and M_{col} indicates the normalized row and column-wise feature vectors obtained by the soft attentive mechanism. Figure 2 represents the architecture of the GAttGAN technique

Loss Function (LF)

For enhancing the accuracy performance, a LF is intended for processing the generator phase. In this framework, the normal and the outcome of the generator are fed as input to the LF, and the error obtained is backpropagated to optimize the model parameters. The LF is the complex in training the network model that affects the robustness and accuracy of the developed model. The objects present in the video frames contain high amounts of unstructured correlated features and dedicated interdependencies. The aim of reconstructing abnormal classes is to generate an outcome more similar to the ground truth. During the actual adversarial process, the generator plans to set classified outcomes more similar to the actual outcome. However, the discriminator fails to differentiate the generated outcome from the actual outcome due to ineffective learning of complicated brain patterns. To tackle this issue, LF is introduced which enhances the accuracy performance. The detailed analysis of the GAN technique is deliberated as follows:

L2 Loss: It isconsidered the default loss function that is caused due to data regularity, differentiability, and convexity. It can be mathematically determined in equation (5),

$$L_2 = \frac{1}{D}\left\| G(x) - x \right\|_2^2 \tag{5}$$

Here, D indicates the dimension of the data, and $G(x)$ represents the data generated during the training process. However, L2 LF inclines to be wedged at local minima and makes the outcome inaccurate.

L1 Loss: It is more operative than L2-LF in minimizing training error and the minimum value of L1 LF is lower than that of L2-LF. It can be expressed mathematically in equation (6),

$$L_2 = \frac{1}{D}\left| G(x) - x \right|_2^2 \tag{6}$$

The total LF for enhancing the GAN model is formulated in equation (7),

$$L_{total} = L_1 + L_2 \tag{7}$$

Finally, the SoftMax classifier effectively classifies the image description by learning the object weights.

Secure Data Transmission using ExP-AES Technique

Encryption techniques are required to provide secure data transfer over IoT networks. The transmitter creates the cipher text and encrypts the message using the recommended ExP-AES approach. The encryption text is sent via the optical line from a source to a destination. The recipient receives the encrypted text and uses the decryption technique. The stage of encryption is precisely inverted during the process of decryption. The encrypted text is decoded by the receiver to expose the initial messages. Secure communication from end to end is enabled by this innovative approach to cryptography. N

The Paillier encryption (PE) approach [31] guarantees that the outcome of decryption is the same as the multiplication or addition of the corresponding plaintexts, even when many encrypted values are multiplied or added together. With the help of this capability, encrypted data can be used for calculations without requiring decryption. The Paillier encryption algorithm requires exponentiation to the power N for both encryption and re-encryption. The exponential expansion of a given baseline to a stochastic power is significantly less than N is permitted across encryption and re-encryption operations with the following modifications to the Paillier technique. The "fixed-based comb strategy" is used to increase performance when there is a fixed base and exponentiations happen as a consequence of the fixed base. Even with the new Decisional Fixed Base (DFB) statement, which is more trustworthy than the DCR assumption, the scheme maintains the homomorphic feature. The efficient decryption mechanism of this technique adopts a distinct perspectives approach, yet it follows an identical procedure as Paillier's effective decryption. The use of Paillier's variant method is insecure due to the initial parameter selection approach and hence proposes a different approach that creates a secure system alternatively. Figure 3 illustrates the Paillier Cryptosystem Process

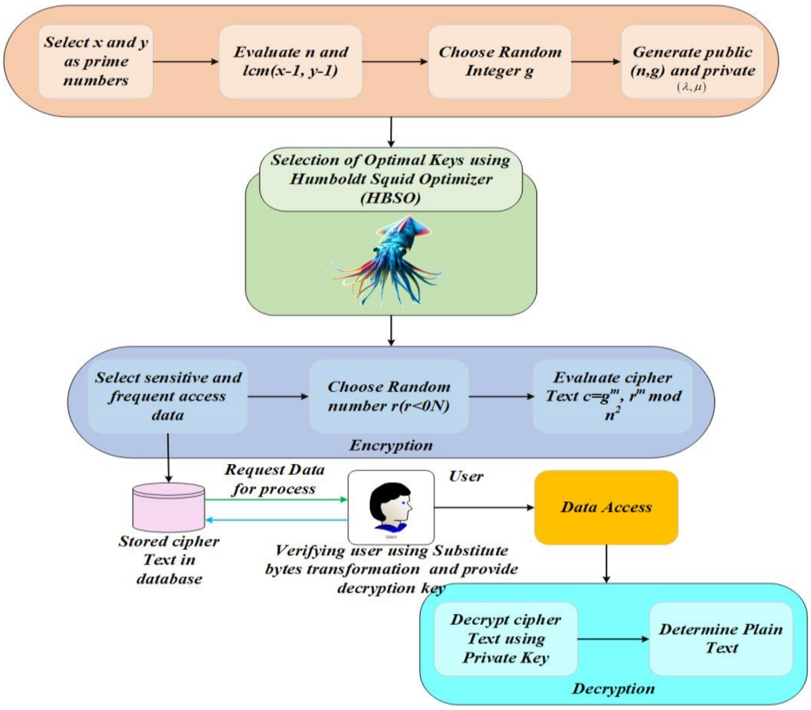
Select x and y as prime numbers
Evaluate n and lcm(x-1, y-1)
Choose Random Integer g
Generate public (n,g) and private (λ, μ)
Selection of Optimal Keys using Humboldt Squid Optimizer (HBSO)
Select sensitive and frequent access data
Choose Random number r(r<0N)
Evaluate cipher Text c=g^m, r^m mod n^2
Encryption
Request Data for process
User
Data Access
Stored cipher Text in database
Verifying user using Substitute bytes transformation and provide decryption key
Decrypt cipher Text using Private Key
Determine Plain Text
Decryption

Figure 3: Paillier Cryptosystem Process

The specific modifications applied to an extended PE method can change depending on the goals and requirements of the adaptation. It is imperative to remember that any changes must be carefully considered and reviewed to ensure they don't introduce vulnerabilities or degrade the security of the initial Paillier system. One of the main advantages of the PE scheme is its homomorphic properties. It enables manipulations on encrypted data without the need for decryption by enabling the ciphertexts to perform homomorphic addition and homomorphic multiplication operations. This feature allows evaluations to be reliably delegated to untrustworthy servers and calculations to safeguard privacy. By preventing an adversary from gaining any insight into the plaintext by examining the corresponding cipher text, it provides semantic security. The approach offers semantic security even though the decisional composite residuality problems that have been reported are challenging. The ciphertext and key sizes for PE are both adjustable. There is support for multiple key sizes, offering various levels of security. This approach may encrypt large communications since the ciphertext's size is linear to the plaintexts. The Paillier scheme, a public-key encryption system, is robust, adaptable, and produces several beneficial properties and results.

Key Generation

The key generation process in the Paillier cryptosystem traditionally involves selecting two large prime numbers x and y to compute the public and private keys. The security of the cryptosystem depends on the difficulty of factoring the product $n = x \times y$and ensuring that the selected primes satisfy certain conditions. Evaluate private key component $\lambda = lcm(x-1, y-1)$ whereas lcm indicates the least common multiple. Then, the random integer g such that $g \in \mathbb{Z}^{*}_{n^2}$ and evaluate private key component μ whereas $\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1}$ and $L(x) = \frac{x-1}{n}$. The public and public keys are deliberated as, (n, g) and (λ, μ) respectively. From the set of public and public keys, optimal sets are considered for the encryption and decryption processes.

Optimal Key Selection Using HBSO Technique

To enhance the security and efficiency of the key selection process, the Humboldt Squid Optimization algorithm [32] can be employed. HBSO is a nature-inspired metaheuristic algorithm based on the foraging behavior of Humboldt squid. It excels in exploring and exploiting search spaces to find optimal private and public keys, making it suitable for selecting primes x and y that not only maximize security but also meet specific cryptographic constraints. The

Humboldt squid (HBS) are bigger and found in the eastern Pacific Ocean. They have excellent biological and economic importance that grows up to 1.5m long and are considered the largest candidate among their family. The velocity of swimming ranges to 24km/h and encompasses the fastest growing species that grows from 1mm to 1 m at 1 to 2 years of age. Their common prey species are shrimps, red crabs, mollusks, tiny squids, pelagic octopuses, amphipods, copepods, etc.

Normally, HBS is capable of flying in multimodal strategies like jetting, roaming, accelerating, gliding, and diving. The other factors of HBS are mating performing internal fertilization and laying millions of eggs over a short lifetime. The HBS are unique predators and the process of attacking, mating and movement are highly the same for determining the global optimal solution for an optimization problem. Here, the weaker squids and school fishes are deliberated as the optimal solution, and inspired by this behavior, the model problem constraints are solved using the HBSO technique. The behavior of the HBSO technique is illustrated in mathematical expression and it is depicted briefly below:

Step 1: Initialization Phase

In the HBSO algorithm, the best individuals are considered the HS, and the remaining are fish. This problem is reliable due to the large body structure and finest fitness compared to school fish.

Step 2: Random Generation

After initiating, arbitrarily choose the most appropriate resolution from the set of input parameters.

Step 3: Fitness Function

The HBSO technique utilized fitness function (FF) for analyzing the optimality of the key selection process and it is formulated in equation (8),

$$f = w_1 \times bit\_length(x) + w_2 \times bit\_length(y) + w_3 \times \mathrm{gcd\_}score(x,y) - \\ w_4 \times size\_difference \tag{8}$$

Here, $bit\_length(x)$, $bit\_length(y)$ indicates the bit lengths of primes x and y, $\mathrm{gcd\_}score(x,y)$ deliberates the Greatest Common Divisor Score for Primes x and y, $size\_difference$ signifies the measure of difference in bit length between x and y, w_1, w_2, w_3 *and* w_4 signifies the weights assigned to each term to balance their importance according to the specific security and efficiency needs.

Step 4: Hunting of Fish schools

The hunting of fish schools is simulated using the mathematical expression determined below:

$$YS^{d}_{new,u} = Y_{best} + J_{jet}\left(-Yf^{d}_{new,r1} - TP^{d}_{r2}\right) \tag{9}$$

Here, $YS^{d}_{new,u}$ indicates the new location of u^{th} HBS in d^{th} dimension, J_{jet} deliberates the locomotive velocity variable, $Yf^{d}_{new,r1}$ signifies the location of $r1^{th}$ fish in d^{th} dimension, and TP^{d}_{r2} defines the stored $r2^{th}$ location in the HBSO memory. Moreover, $r1$ symbolizes the arbitrary integer between fish population and 1, $r2$ signifies the arbitrary integer between 1 and the size of TP.

Step 5: Successful Attack

After changing the updated location, the present position is updated with the new location for HBS YS_u in equation (10),

$$YS_u^v = \begin{cases} YS_u = YS_{new,u} & if \;\; fS_{new,u} < fS_u \\ successful\ escape & otherwise \end{cases} \tag{10}$$

Here, $fS_{new,u}$ and fS_u signifies the FF and present FF of the u^{th} HBS.

Step 6: Successful Escape

After the fish school is attacked by squids, the fish escapes to an arbitrarily positioned location. At this stage, the fish's location and velocity are updated using the expression given below:

$$fS_{new,u} = \begin{cases} Yf_u + \vec{r}_n \times \left(m_{best} - Yf_u \right) f_w, & if \;\; f_e < 0.1 \times \max_{f_e} \\ Yf_u + \vec{r}_n \times \left(AX_{r1} - TP_{r2} \right) f_{w,} & else \end{cases} \tag{11}$$

Here, f_e deliberates the number of present function estimations, $\max_{f_e}$ denotes the number of maximum function estimations, $fS_{new,u}$ indicates the updated location of u^{th} fish, Xf_u encompasses the present location of u^{th} fish, m_{best} signifies the best location, AX_{r1} indicates the r_1^{th} location in the archived best outcome, $\vec{r}_n$ deliberates the arbitrary random vector, $f_w = \frac{f_{best}}{f_u}$ whereas, f_{best} encompasses the best FF, and f_u indicates u^{th} fish.

Step 7: Hunting of larger squids to tiny squids

When the HBS and fish fail to determine a better location at the existing stage, it is considered that there are no more fish to attack. However, the larger HBS hunts the tiny squids and in this phase, the position of HBS is derived mathematically in equation (12),

$$YS^d_{new,u} = YS^d_{new,u} + J_{jet2}\left(-Yf^d_{new,u} - Y^d_{best} \right) \tag{12}$$

Here, J_{jet2} deliberates the second locomotive velocity variable. To define all the best solutions, it is considered that the HBS is in the best location and according to the relationship, the larger squid's movement takes place. Hence, it is assumed that the best location Y_{best} as the tiny HBS.

Step 8: HBS Mating

The generated egg location of HBSO is deliberated by improving the differential evolution mechanism. It can be mathematically formulated in equation (13),

$$\lambda_{eggs} = \left(\theta \times Yf + \left(1 - \theta m_{best} \right) \right) \times \chi + \left(1 - \chi \right) \times P\left(r1,: \right) + w\left(P\left(r3,: \right) - TP\left(r2,: \right) \right) \tag{13}$$

Here, λ_{eggs} indicates the location of HBS egg masses, θ, χ and w deliberates the improved weights for the control search mechanism ranges between 0 and 1. The parameter w can be mathematically formulated in equation (14),

$$w = \max\left(\theta \times \chi\left(1 - \theta \right) \times \chi, 1 - \chi \right) \tag{14}$$

The mathematical expression for the parameter θ and χ can be represented as given below:

$$\theta = \lambda_\theta + x_1 \times z \tag{15}$$

$$\chi = \lambda_\chi + x_2 \times \vec{r}_n \tag{16}$$

Here, x_1 and x_2 represent the constant variables considered during the simulation process. Furthermore, λ_θ and λ_χ defines the vectors having the value 0.5 and it can be mathematically formulated in equations (17-18),

$$\lambda_\theta = \frac{(D_f(Q))(\theta(Q)^2)}{(D_f(Q))(\theta(Q))} \tag{17}$$

$$\lambda_\chi = \frac{(D_f(Q))(\chi(Q)^2)}{(D_f(Q))(\chi(Q))} \tag{18}$$

Here, Q indicates the HBS index that provides a more optimal solution than λ_{eggs}, D_f represents the difference between the fitness of HBS and there λ_{eggs}. However, HBS mate multiple times in their lifetime, the iteration is done several times for the HBSO technique.

Moreover, the parameter χ must be more than zero, and finally, if χ attains zero it can be adjusted using the formulation depicted below:

$$\chi = \lambda_\chi + 0.1 \times \tan(\pi \div rand) \tag{19}$$

Here, $rand$ symbolizes the general arbitrary number ranges between 0 and 1. Finally, the parameter z can be mathematically formulated as,

$$z = \frac{f_e}{Max_{f_e}} \vec{rand}^{10r} \tag{20}$$

Here, $\vec{rand}$ and r defines the general random vector and general random vector ranges between 0 and 1.

Step 9: Control Search Mechanism

The HBSO technique is controlled by different variables such as, J_{jet}, J_{jet2}, z, f_w, θ, χ and w. The parameters J_{jet} and J_{jet2} are contemplated to excite the locomotive shape of HBS and hence, a polynomial function is utilized. The polynomial power function for J_{jet} and J_{jet2} are considered the third and fourth degree respectively. The mathematical expression for J_{jet} and J_{jet2} is depicted below:

$$J_{jet} = (Y - i_1) \times (Y - i_2) \times (Y - i_3) \tag{21}$$

$$J_{jet2} = (Y - i_1) \times (Y - i_2) \times (Y - i_3) \times (Y - i_4) \tag{22}$$

Here, i_1, i_2, i_3 and i_4 indicates the polynomial function that determines the locomotive shape, and Y can be formulated in equation (23),

$$Y = \frac{f_e}{Max_{f_e}} \tag{23}$$

Here, f_e indicates the radius of escaped fish and it is the ratio between the best fitness value and the present fish's fitness value.

Step 10: Return of Optimal Solution

Step11: Termination Criteria

The proposed HBSO technique further iterates into the next stage and the HBSO updating process is repeated from equations (8) to (23) until the termination criteria are satisfied. Subsequently implementing the HBSO algorithm, the best global optimal solution is chosen during repetitive iteration which is utilized as the solution to the problem.

Data Encryption using AES Approach

One of the main objectives of the AES algorithm, which is a block cipher encryption technique, was to replace the DES algorithm following the discovery of several DES algorithm weaknesses. This method's primary objective was to replace the DES method once, once some of its flaws came to light. to create a novel block cipher method that uses a robust and intricate architecture to both encrypt and decrypt data. NIST used three key criteria to assess the techniques offered by cryptographer specialists. NIST solicited renowned experts in data security and encryption to present a special block cipher method for encrypting and decrypting content with strong and intricate architecture.

The AES cipher is repetitive in contrast to the Feistel cipher. It is based on replacement and permutation network (SPN), two popular techniques for data encryption and decryption. Block cipher methods carry out several SPN computations. AES may function with a 128-bit fixed plaintext block size. When working with a matrix of bytes, AES converts the 16 bytes into 4x4 matrices. Another crucial element of AES is the number of rounds. The number of rounds is determined by the key's length. Three separate key dimensions are used by the AES technique to encrypt and decode data. A few basic procedures and tables, such as Sub Word, Root Word, Rcon, MixColumnMatrix, InvMixColumnMatrix, S-box, and Inverse S-Box Tables, form the foundation of this pseudo-code.

These functions and tables are part of the AES protocol and are required for the AES algorithms to function. The underlying design of the AES method consists of several important components and processes. AES operates on data blocks that are typically 128 bits (16 bytes) in size. One common method for shielding data from unwanted access is encryption. The AES technique encrypts data using a predetermined design, providing the highest level of security. Every process uses four components to accomplish this throughout several cycles. The following four processes are used to encrypt a 128-bit block in each cycle. Figure 4 deliberates the Pipeline Structure of the AES technique.

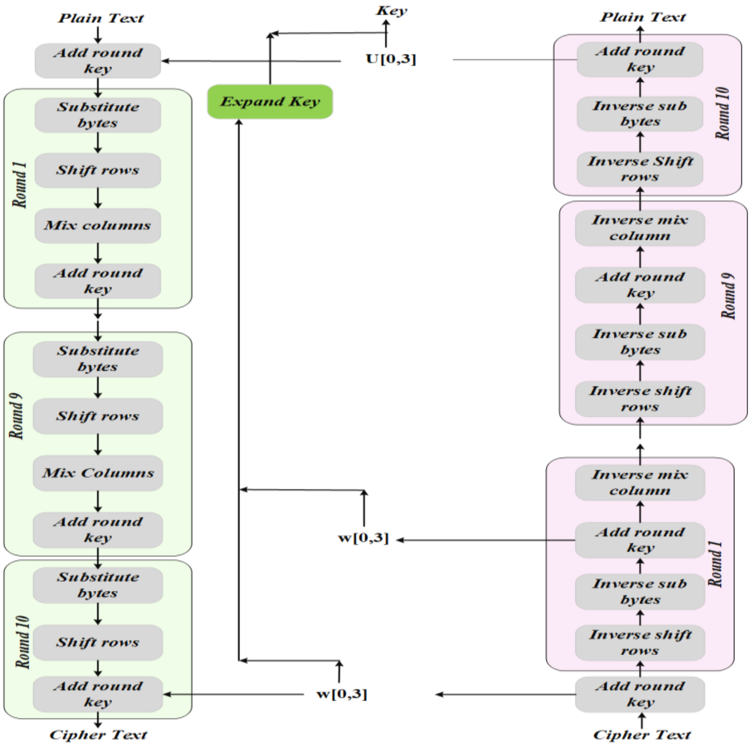

Figure 4: Pipeline Structure of AES technique

Transformation of substitute bytes

A SubBytes transition occurs at the beginning of each cycle. In this step, the state's bytes are switched between using a nonlinear S-box. Diffusion and confusion, two of Shannon's design principles for cryptographic algorithms, are essential to obtaining noticeably higher security. For example, in AES, hexa ED should be used in place of hexa 53 in the state. By combining the digits 5 and 3, ED was created. Apply these procedures to the residual bytes in the state.

Shift Rows Conversion

The process that is applied on the state following SubByte is called ShiftRow. The main goal of this stage is to move the state's bytes from row zero to the left by cycling over each row. This method does not use mutations, and the bytes from row zero remain. Only one bit is rotated left in a circle in the first row. In the second row, there is a two-byte shift to the left. To the left of the final line, three more bytes are inserted.

Add Round Key Conversion

A 4×4 bit grid is used to arrange the input data as well as the key. Compared to AddRoundKey, data encryption can be carried out with far more security. The basis of this process is creating the link between the key and the cipher text. The cipher text originates from the preceding phase. AddRoundKey's performance is directly impacted by the path that users specify. Moreover, the subkey is linked to the stage and state. The primary key is always the source of the secondary key. The sizes of the state and subkey are identical. By bitwise XORing each bit in the state with the corresponding byte of the subkey, the subkey is appended.

Mix Columns Conversion

The state also goes through MixColumn's critical stage. Replication occurs independently of the state. In a matrix conversion, each bit from a row needs to be multiplied by each value (byte) from the state column. Stated differently, the state needs to be multiplied by every row of the matrix transition. With XOR, the result of this multiplier is concatenated to create an additional sequence of four bytes for the next state.

AES Procedure

The decryption procedure is used to return the encrypted data to its original form. The key that was obtained from a message sender serves as the foundation for this process. Both the sender and the recipient of the communication can encrypt and decrypt content using AES, and the decryption process is identical to that of encryption inverted. AES is one of the most powerful procedures that is widely used worldwide in a variety of industries. Compared to DES and 3DES, this method accelerates the encryption and decryption of data. The result of the AES algorithm depends on the specific inputs that are used. On average, AES analyzes data in blocks of 128 bits (16 bytes).

RESULTS AND DISCUSSION

The proposed framework is processed and simulated via the Python platform and a freely accessible NSL-KDD database [28] is utilized for the training process. Several conventional techniques like Deep-LSTM, DNN, RBFN, RNN, and DBN are compared with the proposed technique to prove the efficacy of the proposed scheme. The proposed method is processed under Intel(R) Core (TM) i5-4300M CPU with 4GB installed RAM using a 64-bit operating system. Various assessment measures like accuracy, F-measure, FDR, encryption time, decryption time, conversion time, reliability, security level, and throughput are computed to analyze the performance of the proposed method.

Assessment Measures

Performance indicators like accuracy, F-measure, FDR, encryption time, decryption time, conversion time, reliability, security level, and throughput are scrutinized to better understand the proposed approach.

Accuracy

It determines the model's overall accuracy, accounting for both TP and TN. It is calculated using equation (24),

$$Accuracy = \frac{w+x}{w+x+y+z} \tag{24}$$

F-measure

The F-measure displays the consonant mean of recall and precision. It is computed using equation (25) as follows,

$$F1-score = 2 * \left(\frac{\Pr ecision * \operatorname{Re} call}{\Pr ecision + \operatorname{Re} call} \right) \tag{25}$$

FDR

It is defined as the expected proportion of false positives among all positive results.It is calculated using equation (26),

$$FDR = \frac{z}{z + x} \tag{26}$$

Here, w, x, y, z indicates the TN, TP, FN, and FP respectively.

Encryption Time (ET)

Encryption time refers to the amount of time taken by an encryption algorithm to convert plaintext data into ciphertext. It is calculated using equation (27),

$$T_{encryption} = \frac{D_{data}}{r_{encryption}} + T_{overhead} \tag{27}$$

Here, $T_{encryption}$ indicates the Encryption time, D_{data} deliberates the Size of the data to be encrypted in bits, $r_{encryption}$ signifies the rate of encryption (Bits per second), and $T_{overhead}$ denotes the overhead time.

Decryption Time (DT)

Decryption time refers to the amount of time required by a decryption algorithm to convert ciphertext back into its original plaintext form. It is calculated using equation (28),

$$T_{decryption} = \frac{D_{data}}{r_{decryption}} + T_{overhead} \tag{28}$$

Here, $T_{decryption}$ indicates the decryption time, D_{data} deliberates the Size of the data to be decrypted in bits, $r_{decryption}$ signifies the rate of decryption (Bits per second), and $T_{overhead}$ denotes the overhead time.

Throughput

Throughput refers to the number of packets or amount of data that can be transmitted securely through the IoT network per unit of time. It is calculated using equation (29),

$$Throughput = \frac{Number\ of\ Packets\ Transmitted}{Total\ time\ Taken} \tag{29}$$

Computational Analysis of Proposed Method over Conventional Schemes

In this section, the performance achieved by the proposed method over the existing schemes is deliberated via graphical illustration. Several existing methods like Deep-LSTM, DNN, RBFN, RNN, and DBN techniques are compared with the proposed GAttGAN-ExAES-HBSO technique framework. The detailed analysis of the obtained performance is depicted below.

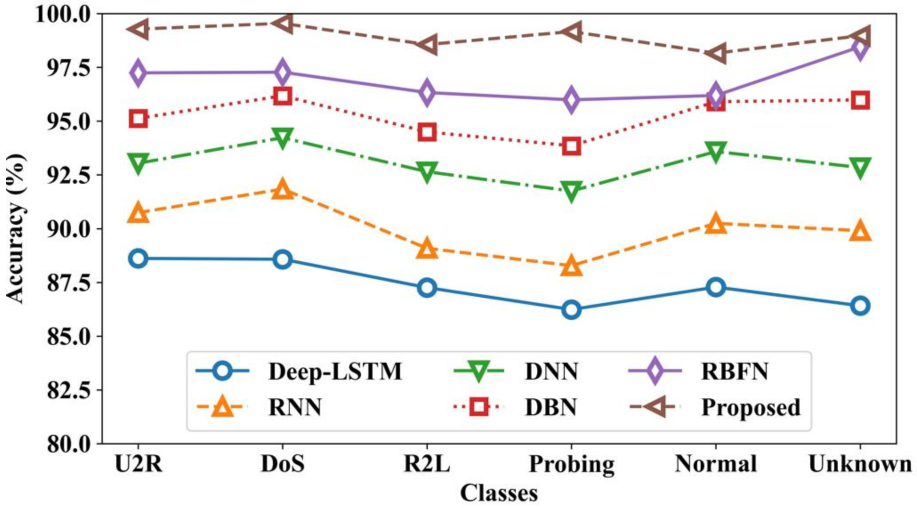

Figure 5: Accuracy Analysis by Varying Classes

Figure 5 deliberates the accuracy analysis by varying classes under different Techniques. The graphical manifestation proved that the suggested model is very effective for promoting security in IoT networks. For existing Deep-LSTM, the accuracy of 88.61%, 88.57%, 87.25%, 86.23%, 87.28%, and 86.41% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing DNN, the accuracy of 93.03%, 94.22%, 92.64%, 91.74%, 93.58%, and 92.84% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing RNN, the accuracy of 90.74%, 91.84%, 89.08%, 88.27%, 90.24%, and 89.90% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing RBFN, the accuracy of 97.24%, 97.27%, 96.32%, 95.98%, 96.19%, and 98.45% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing DBN, the accuracy of 95.12%, 96.17%, 94.49%, 93.84%, 95.89%, and 95.98% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For proposed GAttGAN-ExAES-HBSO, the accuracy of 99.27%, 99.54%, 98.55%, 99.16%, 98.15%, and 98.70% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively.

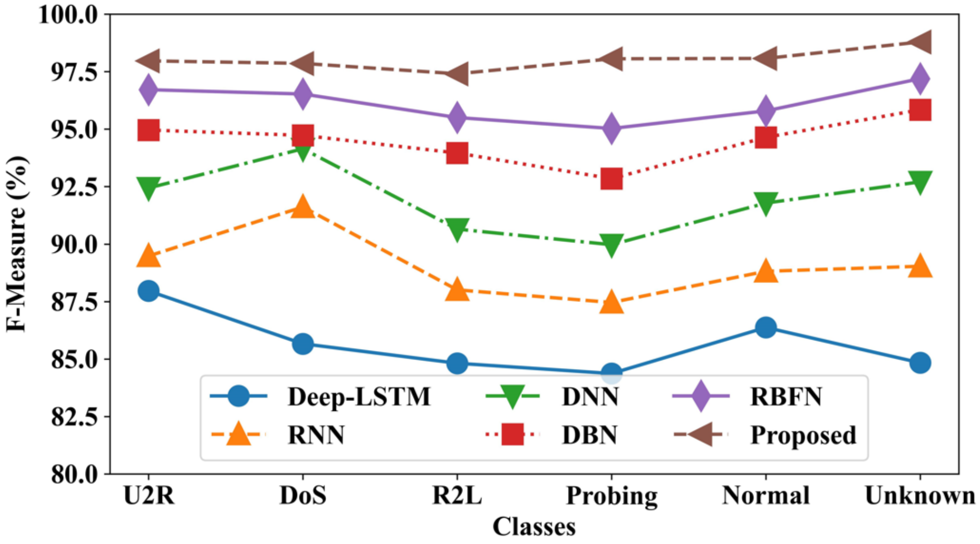

Figure 6: F-measure Analysis by Varying Classes

Figure 6 deliberates the F-measureanalysis by varying classes under different Techniques. The graphical manifestation proved that the suggested model is very effective for promoting security in IoT networks. For existing Deep-LSTM, the F-measure of 87.96%, 85.66%, 84.36%, 86.37%, and 84.83% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing DNN, the F-measure of 92.43%, 94.14%, 90.65%, 89.97%, 91.78%, and 92.70% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing RNN, the F-measure of 89.48%, 91.61%, 88%, 87.45%, 88.81%, and 89.03% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing RBFN, the F-measure of 96.71%, 96.52%, 95.50%, 95.02%, 95.79%, and 97.19% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing DBN, the F-measure of 94.95%, 94.72%, 93.95%, 92.84%, 94.63%, and 95.84% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For proposed GAttGAN-ExAES-HBSO, the F-measure of 97.96%, 97.85%, 97.40%, 98.05%, 98.07%, and 98.78% for U2R, DoS, R2L, Probing, normal, and unknown classes respectively.

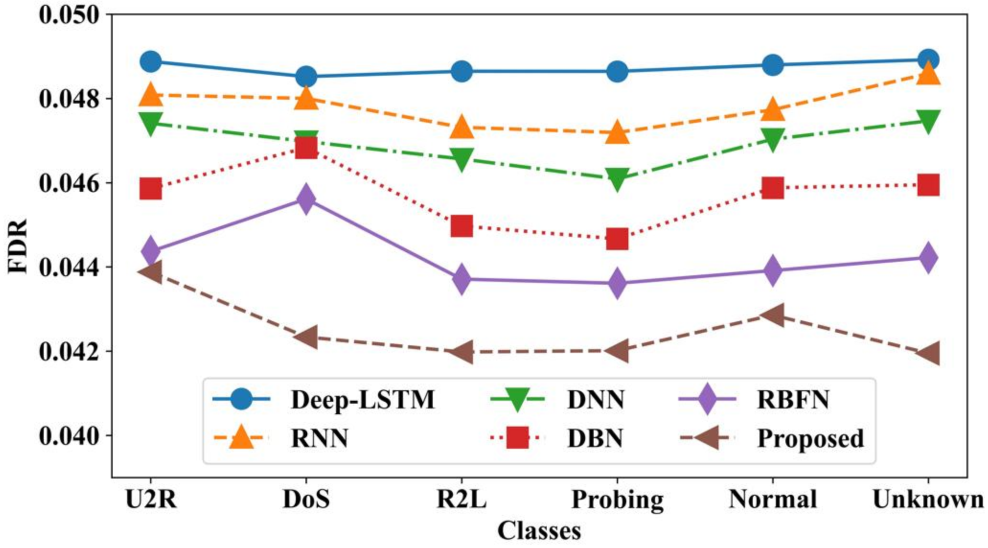

Figure 7: FDR Analysis by Varying Classes

Figure 7 deliberates the FDR analysis by varying classes under different Techniques. The graphical manifestation proved that the suggested model is very effective for promoting security in IoT networks. For existing Deep-LSTM, the FDR of 0.0488, 0.0486, 0.0486, 0.0487, and 0.0489 for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing DNN, the FDR of 0.0474, 0.0469, 0.0465, 0.0460, 0.0470, and 0.0476 for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing RNN, the FDR of 0.04808, 0.0480, 0.0473, 0.0471, 0.0471, 0.0477, and 0.0485 for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing RBFN, the FDR of 0.044, 0.0456, 0.0419, 0.0420, 0.0428, and 0.0419 for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For existing DBN, the FDR of 0.0458, 0.0468, 0.0449, 0.0446, 0.0458, and 0.0459 for U2R, DoS, R2L, Probing, normal, and unknown classes respectively. For proposed GAttGAN-ExAES-HBSO, the FDR of 0.0438, 0.0423, 0.04198, 0.0420, 0.0428, and 0.0481 for U2R, DoS, R2L, Probing, normal, and unknown classes respectively.

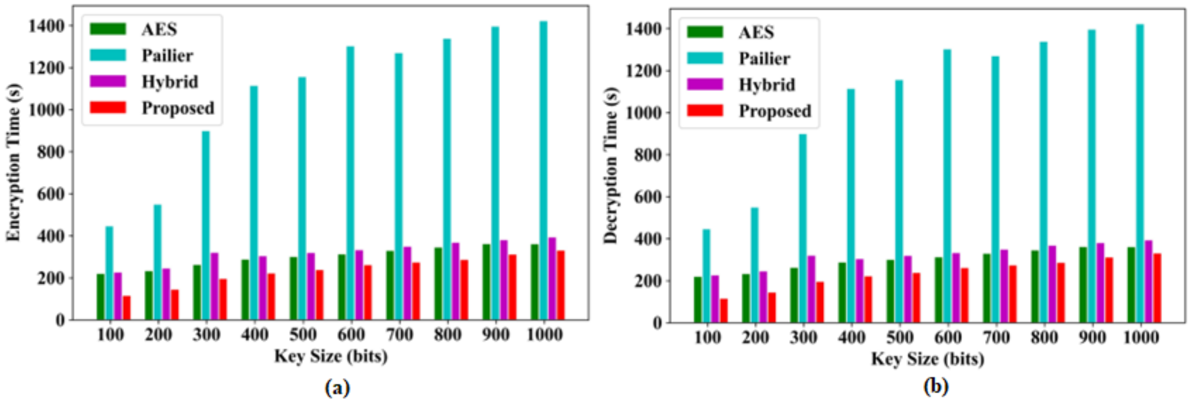

Figure 8: Encryption Time Analysis by Varying Key Size

Figure 8 deliberates the encryption time analysis by varying key sizes. The graphical manifestation proved that the suggested model is very effective in minimizing the encryption time in IoT networks.For 100-bit Key size, the existing AES, Paillier, Hybrid P-AES, and proposed HBSO-ExPAES obtained an ET of 221.94s, 441.16s, 228.32s, and 117.25s respectively. For 1000-bit Key size, the existing AES, Paillier, Hybrid P-AES, and proposed HBSO-ExPAES obtained an ET of 362.50, 1423.65s, 395s, and 332.91s respectively. In the case of decryption time, the conventional techniques consume time and are less capable in the data security process. For 100-bit Key size, the existing AES, Paillier, Hybrid P-AES, and proposed HBSO-ExPAES obtained a DT of 221.94s, 447.16s, 228.32s, and 117.25s respectively. For 1000-bit Key size, the existing AES, Paillier, Hybrid P-AES, and proposed HBSO-ExPAES obtained a DT of 362.50s, 1423.65s, 395s, and 332.91s respectively.

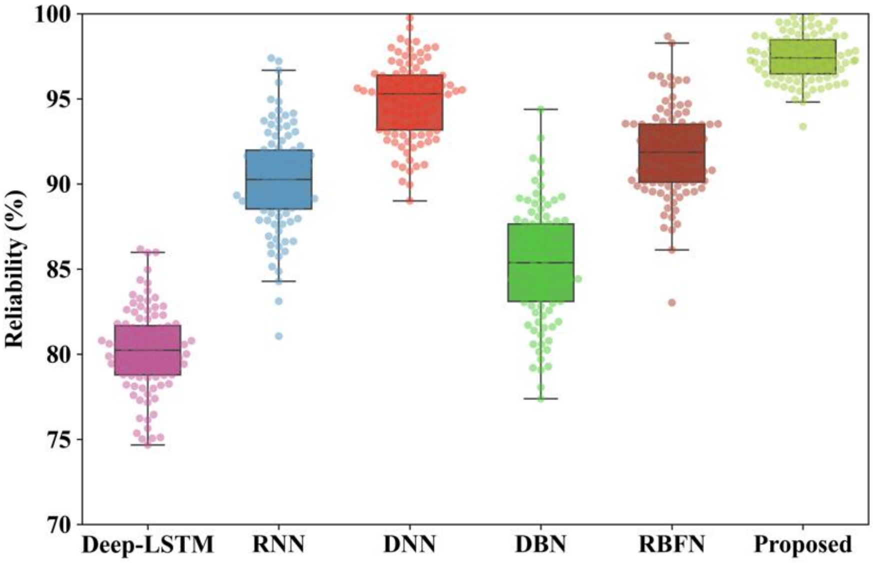

Figure 9: Reliability Analysis by Varying Existing Schemes

Figure 9 indicates the reliability analysis by varying existing schemes. On analyzing the reliability performance in the graph, it is clear that the proposed GAttGAN-ExAES-HBSO technique performs more effectively than other techniques. The existing Deep-LSTM, RNN, DNN, DBN, RBFN, and proposed GAttGAN-ExAES-HBSO techniques obtained the reliability of 80%, 90%, 95%, 85%, 92%, and 98.6% respectively.

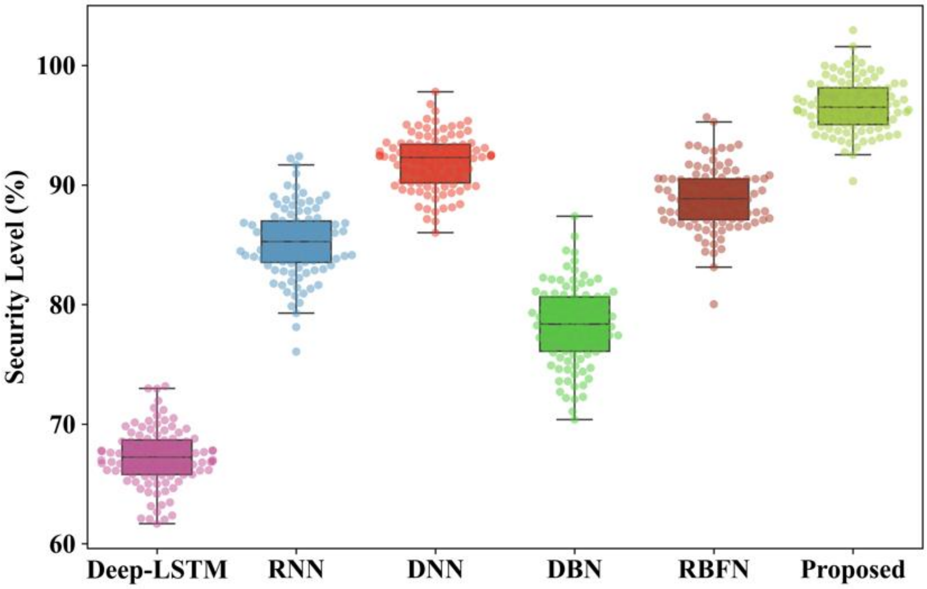

Figure 10: Security Level Analysis by Varying Existing Schemes

Figure 10 indicates the security analysis by varying existing schemes. On analyzing the security level performance in the graph, it is clear that the proposed GAttGAN-ExAES-HBSO technique has more effective performance than other techniques. The existing Deep-LSTM, RNN, DNN, DBN, RBFN, and proposed GAttGAN-ExAES-HBSO techniques obtained the security level of 67%, 85%, 92%, 78%, 89%, and 96.8% respectively.

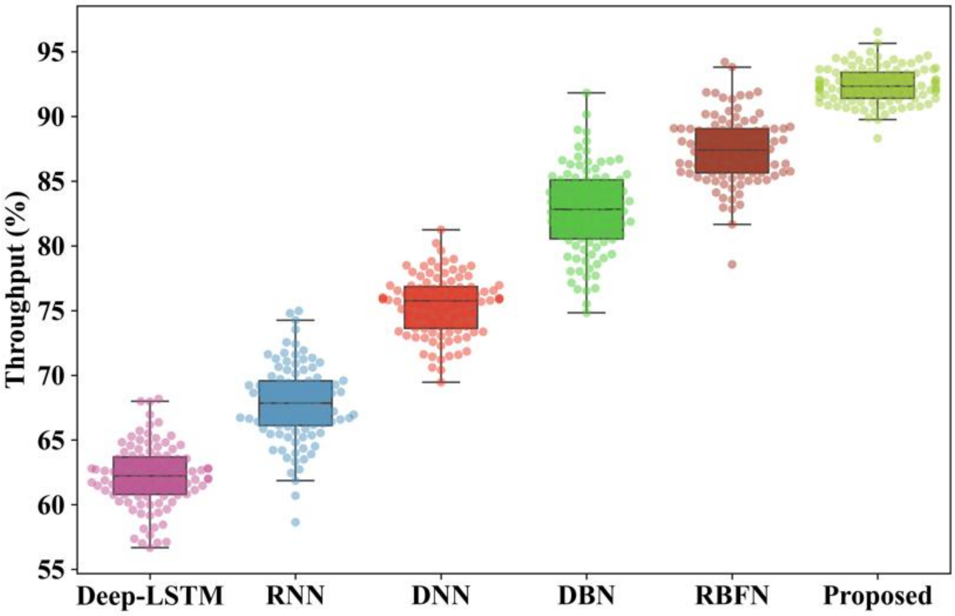

Figure 11: Throughput Analysis by Varying Existing Schemes

Figure 11indicates the throughputanalysis by varying existing schemes. On analyzing the throughput performance in the graph, it is clear that the proposed GAttGAN-ExAES-HBSO technique effective performance than other techniques. The existing Deep-LSTM, RNN, DNN, DBN, RBFN, and proposed GAttGAN-ExAES-HBSO techniques obtained the throughput of 62.4%, 67.58%, 75.45%, 82.45%, 91.23%, and 95.72% respectively.

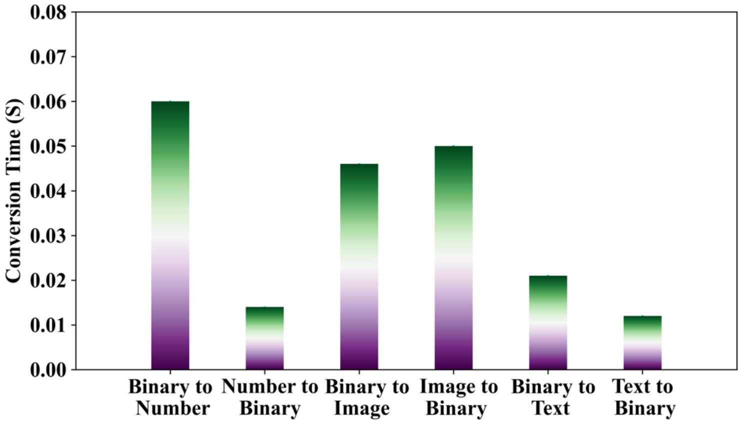

Figure 12: Conversation Time Analysis of the Proposed Framework

Figure 12encompasses the conversation time analysis of the proposed framework. The figure displays a bar chart comparing the conversion times (in seconds) for various data types, including Binary to text, text to binary, binary to image, binary to number, binary to text, and binary to number. Among these, the binary-to-number conversion takes the longest time, while text-to-binary conversion is the fastest. This analysis highlights the efficiency of data processing in the proposed security framework. The efficacy of the encryption and decryption operations is greatly increased by the enhanced data conversion methods of the suggested technology. This decrease in conversion time makes the system more responsive and increases overall performance, which makes it especially suitable for safe and effective IoT environments. The method guarantees that IoT security frameworks can match the demands of contemporary, dynamic IoT networks by enabling speedier real-time processing and providing a reliable solution for protecting sensitive data.

CONCLUSION

The proposed framework introduced and investigated a novel attack detection framework and improved encryption scheme for secure data transmission in IoT networks. The framework begins with the preprocessing of raw data from the NSL-KDD dataset using a variable stability scaling (Var-SS) technique, which ensures high-quality data normalization. Then, the Guided Attentional Generative Adversarial Network (GAtt-GAN), is introduced that accurately identifies and classifies various types of malware attacks, including U2R, DoS, R2L, and Probing, as well as normal and unknown threats. The Extended Paillier-boosted Advanced Encryption Standard (ExP-AES) technique, combines the strengths of the Paillier cryptosystem and AES algorithm. The Paillier system's homomorphic properties allow encrypted data to be manipulated without decryption, enhancing security and efficiency. Moreover, the Humboldt Squid Optimizer (HBSO) dynamically selects AES encryption keys, increasing the encryption process's unpredictability and resilience against cryptographic attacks. The novel GAtt-HBSO-ExPAES technique introduces significant improvements to traditional cryptographic methods, addressing potential vulnerabilities and fortifying data security.The proposed framework is simulated via the Python platform and a freely accessible NSL-KDD database is utilized for the attack classification framework. Various performance measures are analyzed, like encryption time, decryption time, throughput, accuracy, F-measure, false discovery rate (FDR), reliability, security level analysis, encryption, and decryption time, and compared with the proposed framework to prove the model's efficacy. The overall accuracy of 98.5%, F-measure of 98.07%, and FDR of 0.042, encryption and decryption time of 117.5s are obtained by the proposed framework for providing security against IoT vulnerabilities. Although the framework aims to detect various malware attacks, it may not cover all possible attack types, especially emerging or novel attacks that are not well-represented in the dataset. In the future, the proposed framework will be extended by ensuring compatibility with different IoT platforms and standards, facilitating wider adoption of the framework across various sectors.

REFERENCES

[1] Thabit, Fursan, Ozgu Can, Sharaf Alhomdy, Ghaleb H. Al-Gaphari, and Sudhir Jagtap. "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing." International Journal of Intelligent Networks 3 (2022): 16-30.

[2] Mahlake, Ntebatseng, Topside E. Mathonsi, Deon Du Plessis, and Tonderai Muchenje. "A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things." J. Commun. 18, no. 1 (2023): 47-57.

[3] Sudhakaran, Pradeep. "Energy efficient distributed lightweight authentication and encryption technique for IoT security." International Journal of Communication Systems 35, no. 2 (2022): e4198.

[4] Hintaw, Ahmed J., Selvakumar Manickam, Shankar Karuppayah, Mohammad Adnan Aladaileh, Mohammed Faiz Aboalmaaly, and Shams UlArfeen Laghari. "A robust security scheme based on enhanced symmetric algorithm for MQTT in the Internet of Things." IEEE Access 11 (2023): 43019-43040.

[5] Tharakan, Linoy A., Sherly Daniel, and R. Dhanasekaran. "Security enhancement and monitoring for data sensing networks using a novel asymmetric mirror-key data encryption method." AI and Machine Learning Paradigms for Health Monitoring System: Intelligent Data Analytics (2021): 65-78.

[6] Nagaraj, S., Atul B. Kathole, Leena Arya, Neha Tyagi, S. B. Goyal, Anand Singh Rajawat, Maria Simona Raboaca, Traian CandinMihaltan, Chaman Verma, and George Suciu. "Improved secure encryption with energy optimization using random permutation pseudo algorithm based on internet of thing in wireless sensor networks." Energies 16, no. 1 (2022): 8.

[7] Ashraf, Zeeshan, Adnan Sohail, and Muhammad Yousaf. "Robust and lightweight symmetric key exchange algorithm for next-generation IoE." Internet of Things 22 (2023): 100703.

[8] Panahi, Uras, and Cüneyt Bayılmış. "Enabling secure data transmission for wireless sensor networks based IoT applications." Ain Shams Engineering Journal 14, no. 2 (2023): 101866.

[9] Bian, Qingquan, Yue Zhang, Chang Song, and Axin Wu. "Flexible symmetric predicate encryption for data privacy in IoT environments." Peer-to-Peer Networking and Applications 17, no. 2 (2024): 656-664.

[10] Sumathi, M. S., Vipin Jain, G. Kalyan Kumar, and Zarrarahmed Z. Khan. "Using Artificial Intelligence (AI) and Internet of Things (IoT) for Improving Network Security by Hybrid Cryptography Approach." (2023): 1133-1139.

[11] Sekar, C., Vinod Ramesh Falmari, and M. Brindha. "Secure IoT-enabled sharing of digital medical records: An integrated approach with reversible data hiding, symmetric cryptosystem, and IPFS." Internet of Things 24 (2023): 100958.

[12] Bandaru, Venkata Naga Rani, VSH Gayatri Sarman Kaligotla, Uddarraju Dhana Satya Prathap Varma, KanthetiPrasadaraju, and S. Sugumaran. "A Enhancing Data Security Solutions for Smart Energy Systems in

IoT-Enabled Cloud Computing Environments through Lightweight Cryptographic Techniques." In IOP Series: Earth and Environmental Science, vol. 1375, no. 1, p. 012003. IOP Publishing, 2024.

[13] Kumar, Mukesh, Monika Sethi, Shalli Rani, Dipak Kumar Sah, Salman A. AlQahtani, and Mabrook S. Al-Rakhami. "Secure Data Aggregation Based on End-to-End Homomorphic Encryption in IoT-Based Wireless Sensor Networks." Sensors 23, no. 13 (2023): 6181.

[14] Justindhas, Y., and P. Jeyanthi. "Secured model for internet of things (IoT) to monitor smart field data with integrated real-time cloud using lightweight cryptography." IETE Journal of Research 69, no. 8 (2023): 5134-5147.

[15] Namasudra, Suyel. "A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure." Computers and Electrical Engineering 104 (2022): 108426.

[16] El-Shafai, Walid, Ahmed K. Mesrega, Hossam Eldin H. Ahmed, Nirmeen A. El-Bahnasawy, and Fathi E. Abd El-Samie. "An efficient multimedia compression-encryption scheme using latin squares for securing internet-of-things networks." Journal of Information Security and Applications 64 (2022): 103039.

[17] Hasan, Mohammad Kamrul, Muhammad Shafiq, Shayla Islam, Bishwajeet Pandey, Yousef A. Baker El-Ebiary, Nazmus Shaker Nafi, R. Ciro Rodriguez, and Doris Esenarro Vargas. "Lightweight cryptographic algorithms for guessing attack protection in complex internet of things applications." Complexity 2021, no. 1 (2021): 5540296.

[18] Subashini, Arasada, and P. Kanaka Raju. "Hybrid AES model with elliptic curve and ID based key generation for IOT in telemedicine." Measurement: Sensors 28 (2023): 100824.

[19] Saleh, Matasem, Noor Zaman, Azween Abdullah, and Raazia Saher. "Message security level integration with iotes: A design dependent encryption selection model for iot devices." Int. J. Comput. Sci. Netw. Secur.(IJCSNS) 22 (2022): 328.

[20] Hameedi, Saleem S., and Oguz Bayat. "Improving IoT data security and integrity using lightweight blockchain dynamic table." Applied Sciences 12, no. 18 (2022): 9377.

[21] Chen, Dajiang, Hao Wang, Ning Zhang, Xuyun Nie, Hong-Ning Dai, Kuan Zhang, and Kim-Kwang Raymond Choo. "Privacy-preserving encrypted traffic inspection with symmetric cryptographic techniques in IoT." IEEE Internet of Things journal 9, no. 18 (2022): 17265-17279.

[22] Das, Sangjukta, and SuyelNamasudra. "A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure." Computers and Electrical Engineering 101 (2022): 107991.

[23] Rupa, Ch, Greeshmanth, and Mohd Asif Shah. "Novel secure data protection scheme using Martino homomorphic encryption." Journal of Cloud Computing 12, no. 1 (2023): 47.

[24] Abroshan, Hossein. "A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms." International Journal of Advanced Computer Science and Applications 12, no. 6 (2021).

[25] Jalasri, M., and L. Lakshmanan. "Managing data security in fog computing in IoT devices using noise framework encryption with power probabilistic clustering algorithm." Cluster Computing 26, no. 1 (2023): 823-836.

[26] Umapathy, B., and G. Kalpana. "A novel symmetric cryptographic method to design block complexity for data security." Computers and Electrical Engineering 104 (2022): 108467.

[27] Al-Shargabi, Bassam, Rame Jamil Al-Dwairi, and Mohammed Abbas Fadhil Al-Husainy. "Using DNA to develop a lightweight symmetric encryption method to encrypt the data of IoT devices." International Journal of Electronic Security and Digital Forensics 16, no. 2 (2024): 173-189.

[28] https://www.kaggle.com/datasets/hassan06/nslkdd

[29] D. Singh and B. Singh, “Investigating the impact of data normalization on classification performance,” Applied Soft Computing, vol. 97, p. 105524, Dec. 2020.

[30] Huo, Xiaofei, Bin Jiang, Haotian Hu, Xinjiao Zhou, and Bolin Zhang. "OSAGGAN: one-shot unsupervised image-to-image translation using attention-guided generative adversarial networks." International Journal of Machine Learning and Cybernetics 14, no. 10 (2023): 3471-3482.

[31] Chen, Wei, Zidong Wang, Quanbo Ge, Hongli Dong, and Guo-Ping Liu. "Quantized Distributed Economic Dispatch for Microgrids: Paillier Encryption–Decryption Scheme." IEEE Transactions on Industrial Informatics (2024).

[32] Anaraki, Mahdi Valikhan, and Saeed Farzin. "Humboldt Squid Optimization Algorithm (HSOA): A novel nature-inspired technique for solving optimization problems." IEEE Access 11 (2023): 122069-122115.