International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

Cryptographic Framework of Attack Detection and Secure Data Transmission in IoT

Ranjith J[1], Mahantesh K[2] , Abhilash C N[3]

[1] Information Science and Engineering, SJB Institute of Technology, Bengaluru, India
[2]Electronics and Communication Engineering, SJB Institute of Technology, Bengaluru, India
[3] Information Science and Engineering, SJB Institute of Technology, Bengaluru, India
Visvesvaraya Technological University, Belagavi

E-mail address: ranjith.krnagar@gmail.com, mahantesh.sjbit@gmail.com, cnabhilash1@gmail.com

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: In the present era, the number of Internet of Health Things (IoHT) devices and applications has drastically expanded. Security and attack are major issues in the IoHT domain because of the nature of its architecture and sorts of devices. Over the recent few years, network attacks have dramatically increased. Many detection and encryption techniques are there in the literature, but they lack accuracy, training stability, insecurity, delay etc. By the above concerns, this manuscript introduces a novel deep learning technique called Agnostic Spiking Binarized neural network with Improved Billiards optimization for accurate detection of network attacks and Light Weight integrated Puzzle War Elliptic Curve Cryptographic framework for secure data transmission with high security and minimal delay. Optimal features from the datasets are selected by volcano eruption optimization algorithm with better convergence for reducing the overall processing time. Wilcoxon Rank Sum and Mc Neymar's tests are performed for proving the statistical analyses. The outcomes show that the introduced approach performs with an overall accuracy of 99.99% which is better than the previous techniques demonstrating the effectiveness.

Keywords: *Internet of Things, Deep Learning, Attack Detection, Secure Data Transmission, Cryptographic Framework, Encryption and Decryption.*

1. INTRODUCTION

One of the advanced technologies known as the IoT enables autonomous devices, equipment, sensors, robotic systems, IOHT and actuators [1]. The quality, efficiency, and productivity of work are greatly improved by IoT networks, which also provide significant financial gains. [2]. IoT devices form a vast network that is linked to distinct from the present Internet. But the accompanying security and privacy solutions cannot retain the expansion of IoT devices [3]. In the majority of Internet-based scenarios, devices communicate with apps that are operated remotely via the network, which makes it possible for hostile agents to take over devices [4].

In various fields of health care, IoT is widely implemented. The risk of security ruins in IOHT is caused during data transmission and reception. Internet is vulnerable to various kinds of cyber-attacks in medical field like Denial-of-Service (DoS), Address Resolution Protocol (ARP) spoofing and treatment manipulation in IoHT environments etc. Attackers pay attention to the big commercial market as well. The intruders seek to investigate and initiate attacks in networks of IoHT, which may result in massive financial loss for the companies that depend on those services, impacting global audience, commercial portals like GitHub, and posing a heavy risk to security and privacy [5]. But it's difficult to offer complete security and privacy options for IoT networks because of their specific features [6].According to the 2023 statistics report, the growth rate of network attacks has been rapidly rising over the previous six years as shown in Figure 1.

Based on this report, it is inferred that security risks significantly affect mission-critical programs utilized in regular company operations [7]. It is vital to use more rapid and efficient detection methods as network attacks proliferate and network data volumes dramatically increase [8].

E-mail:ranjith.krnagar@gmail.com

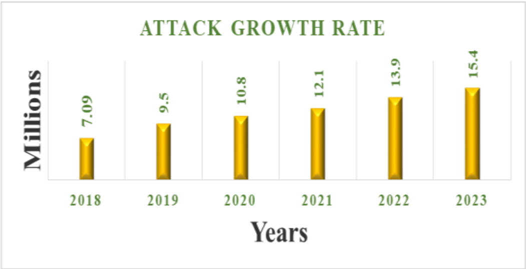

Figure 1. Attack growth rate

Currently, the majority of existing detection techniques make use of the conventional attack detection paradigm without taking into account the specific features of IoT domains. The variety of attack interfaces is generally not properly considered by detection techniques and is also not responsible to low rate attacks [9]. Additionally, these technologies are incapable of responding to learning-automation threats in the IoHT [10]. In response to this issue, this manuscript proposes a lightweight cryptography framework that is further susceptible to minimal computational cost and minimal-rate attacks. This model is a deep learning based secure data transmission and detection.

2. LITERATURE REVIEW

Most probably, several machine learning and deep learning had great influence in attack detection, key generation, data transmission, network security, energy efficiency and privacy in IoT and Wireless Sensor Networks (WSN). In 2022, Justindhas Y and Jeyanthi P [11] provided a hybridization of the SCADA technique's attack detection with Recurrent Neural Networks (RNN) and normalized K-means grouping. A combination of classification and attack detection approaches are employed to reduce the feature's complexity. Through the use of elephant herding optimization, the finest features are chosen. Caesar ciphering is employed to resist attacks, while enhanced elliptic curve cryptography is utilized to raise the level of safety. This approach experienced issues with gradient inflating and vanishing, and training is a difficult task. Also, an effective attack detection model in cloud is created by Aouedi O et al. [12] in 2022 using a federated Semi-Supervised Learning (SSL) method with labelled and unlabeled information. On each device, an auto encoder is trained to find the relevant and minimal-dimensional attributes. The cloud server lastly constructs a supervised network by combining the fully connected layers to the global aggregator, trains the method using openly accessible labelled data, and then terminates the process. Both the training and detection of this technique require extensive computing, which takes time. In 2022, Gudla SP et al. [13] suggested a DDoS attack detection system for fog-based applications in IoT using Deep Intelligent (DI). To predict the end IoT device performance, DI approach is fixed on the computation module of the fog node. The evaluation is done on Deep Neural Multi-Layer Perceptron (DNMLP) and Long Short Term memory (LSTM) techniques along with the conventional ML techniques like Support Vector Machine, K-Nearest Neighbors, Logistic Regression, and Random Forest for the selection of the best DI approach. This DI technique possess a degradation problem and training instability. It is also essential to identify the attacks in smart cities. Therefore, a Modified Adaptive Neuro-Fuzzy Inference System (MANFIS) and Improved Rivest Shamir Adleman (IRSA) was developed by Duraisamy A and Subramaniam M [14] in 2022 for detecting attacks in smart cities and for transmitting data securely. The user receives the non-attacked data securely and then the data is decrypted. The decrypted data is then estimated for more analysis. Since encryption requires both the even and uneven key, this method occasionally fails.

In 2023, Alabsi BA et al. [15] suggested a dual CNN approach for attack detection on IoT networks. This approach uses BoT IoT dataset. The finest features from the input data are chosen by leveraging the first CNN. Second CNN performs effective detection based on the first CNN's output. Although, this method faces maximized complexity and more requirements of resources, weak optimization of parameter. To find intrusion in the Health Care (HC) scheme, a combination of deep sparse auto encoder and also the Bidirectional Long Short-Term Memory (Bi-LSTM) framework is built by Kumar P et al. [16] in 2023. This work also developed a zero-knowledge proof strategy-based Blockchain-orchestrated Deep Learning (DL) technique for integrating and transmitting data securely in an IoT-enabled Health Care (HC) scheme. In order to solve issues with data storage expenses and security, this technique also interfaces with the inter planetary file model, and Ethereum smart transactions. The test results demonstrate that this technology is ineffective for transmitting secure data. Another approach by Priyadarshini I et al. [17] also developed an attention-based Bi-LSTM integrated with CNN (Bi-LSTM CNN) for DDoS attacks identification in application layer. The network failure due to the increased network bandwidth is eliminated by suggested technique. To further enhance the network performance, optimization algorithms is recommended with Bi-LSTM CNN. In 2023, Vijayakumar KP et al. [18] utilized an Edith Cowan University-Internet of Health Things (ECU-IoHT) dataset for cyber-attack-based detection system. The detection was performed using a Deep Neural Network (DNN) by employing artificial intelligence. However, this process has poor scalability in detecting various attacks. In 2023, Ezhilarasi et al. [19] developed a

Fuzzy and feed-forward neural networks (FFNN) for detecting routing attacks in WSN. But this model requires an integration with optimization algorithms for enhancing performance with limited computational time.

The above reviewed works had several problems without any optimization algorithms. Therefore, Thulasi T and Sivamohan K [20] in 2023 utilized a Light Spectrum Optimizer (LSO) with Multi-Step Convolutional neural network Stacked Long short-term memory (MSCSL) architecture for detecting attacks in IoHT system. The hyper parameter of MSCSL are optimized using LSO. The complexity is reduced and the data adaptability is enhanced with replacing the Rectified Linear Unit (ReLU) by leaky learnable ReLU (LeLeLU). This method faces challenges in real-time implementation due to deployment and privacy issues. Another optimization strategy based effective data transmission was presented by Sankaran KS and Kim BH [21] in 2023 for outlier detection in IoT. Robust Multi-Cascaded CNN (RMC-CNN) is integrated with multi scale Grasshopper Optimization Algorithm (GOA) for detecting the attack types. A Dynamic Honey Pot Encryption (DHPE) algorithm is used for generation of key, secure transmission and decryption. The deviation in IoT network caused by inverse behavior of microservices at several durations is weakly handled by this suggested model which led to increased anomalies.

The problems from the existing techniques are displayed in Table 1

TABLE I. TABLE TYPE STYLES

Techniques	Existing limitations
[11] SCADA with RNN and normalized K-means clustering	▪ Gradient inflating ▪ Vanishing problem ▪ Training instability in RNN
[12] SSL	▪ High end-to-end delay because both training and detection of this technique require extensive computing
[13] DI	▪ Degradation problem ▪ Training instability of neural network
[14] MANFIS with IRSA	▪ Poor key generation ▪ Insecurity

3. RESEARCH AND METHODS

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

In this section, the proposed approach on accurate and efficient attack detection using ASB-IB and secure data transmission using LW-PWECC is explained in detail. Figure 2 depicts the work flow of introduced technique.

Preprocessing of the input, selecting optimal features using VEA, attack detection using ASB-IB and transmission of data are the various stages of introduced method.

A. Input acquisition and Pre-processing

The input data for Attack Detection (AD) in IoHT is provided by ECU-IoHT dataset. The ECU-IoHT dataset strengthens cyber security of IoHT and aids the security community of healthcare. Therefore, this research work uses this dataset for detecting various cyber-attacks in IoHT [22]. The preprocessing of the IoHT data involves crisp data conversion, splitting and normalization [23].

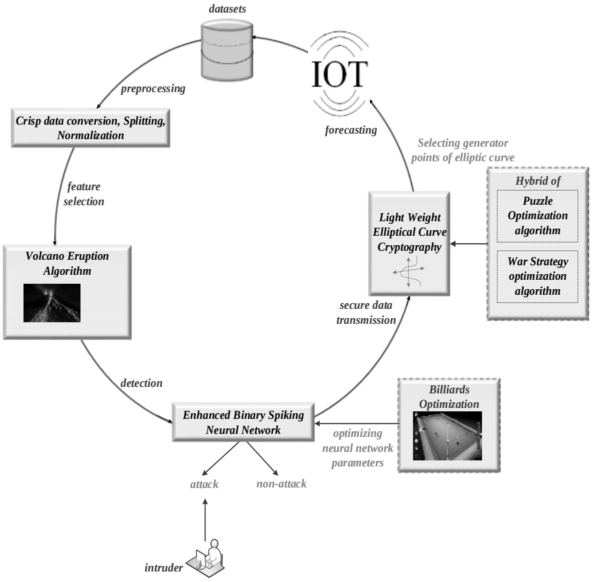
datasets
IOT
preprocessing
Crisp data conversion, Splitting, Normalization
forecasting
Selecting generator points of elliptic curve
feature selection
Hybrid of
Puzzle Optimization algorithm
War Strategy optimization algorithm
Light Weight Elliptical Curve Cryptography
Volcano Eruption Algorithm
secure data transmission
detection
Billiards Optimization
Enhanced Binary Spiking Neural Network
optimizing neural network parameters
attack
non-attack
intruder

Figure 2: Work flow of proposed approach

Crisp data conversion

The input data is transformed into crisp data. Crisp data is defined as data that includes some string values. During the crisp data conversion, the string values are changed as integers.

Splitting

After crisp data conversion, the crisp data is splitted into five types i.e. DoS, ARP spoofing, Network mapper (Nmap) port scan, Smurf attack and Non-Attack.

$$N_d = \left(\frac{(i_d - i_{dMIN})}{(i_{dMAX} - i_{MIN})} \right) \tag{1}$$

where i_d, i_{dMIN}, i_{dMAX}, refers the input , lowest and highest values of the data.

From this preprocessed output, important features are selected by Volcano Eruption Optimization (VEO) algorithm for better classification.

B. *Volcano Eruption Optimization based feature selection*

VEO is motivated from the behavior of volcano [24]. The stepwise procedure of selecting best features for attack detection is given in Table 2.

The best features are selected using the VEO algorithm and the features are classified as with attack and non-attack data using ASB-IB.

TABLE 2: STEPWISE PROCEDURE FOR FEATURE SELECTION

Input: Preprocessed output **Output: Feature selection**
Generate initial populations n : number of solutions p : given positive number for $i = 1 to n$ do Randomly generate solution of populations C : random number D_{rj} : j^{th} random direction Calculate the fitness function The solutions of current populations are exploded and erupted for selecting best features. end for

C. *Attack Detection*

Agnostic Spiking Binarized Neural Network (ASBNN)

The selected features are inputted to the ASBNN classifier which is the modified form of Binarized Spiking Neural Network (BSNN) for detecting DoS, ARP spoofing, NMAP port scan and Smurf attack and Non attack data. The framework of proposed ASB neural network is displayed in Figure 3.

In the training process, the binarized weights are signified in bipolar setup. The membrane potential U_i^{TL} f for ith neuron at time step *t* in layer *l* is defined in equation 2.

$$U_i^{T,L} = U_i^{T-1,L} + \frac{\mu}{\rho}\left(\sum_{j=1}^{m} W_{ij}^{L} \cdot S_j^{T,L-1} - \alpha\right) + \beta \qquad (2)$$

The scaling and shifting parameters are represented as μ and β . ρ and α is denoted as standard deviation of mean of ASBNN. The presynaptic spikes and j^{th} the neuron's presynaptic spikes are denoted as m and $S_j^{T,L-1}$. $W_{ij}^{L} = a * W_{ij}^{B,L}$ is the latent weight and $W_{ij}^{B,L} = sign\left(W_{ij}^{L}\right)$ is the binary weight of ASBNN. Where, $a = \left|W_{ij}^{L}\right|$ the scaling factor of latent weight.

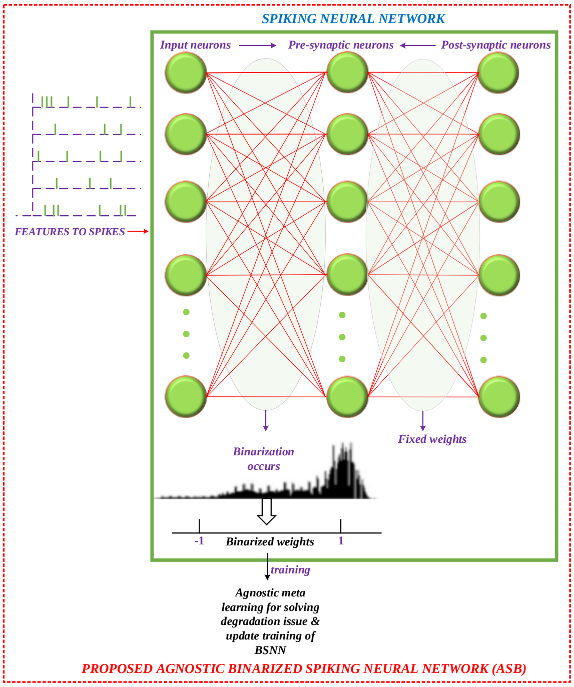

Figure 3: Architecture of proposed neural network

Particularly, a Poisson random number generator is used to convert the actual data input into spike form. The value that is produced is directly related to the sum of spikes with time steps T . Equation 2 generates a membrane potential $U_i^{T,L}$ greater than the firing threshold $\theta_i^{T,L}$ .Following equation 3 uses the final output membrane potential $U_i^{T,L}$, to construct the cross-entropy loss function.

$$l_f = -\sum_{i=1}^{c} Y_i \log\left(\frac{E^{U_i^{T,L}}}{\sum_{k=1}^{c} E^{U_k^{T,L}}}\right) \qquad (3)$$

where, c is the overall network outputs and $Y_i = (y1, y2, ..., yc)$ is a label vector

$$\cdot\ W_{ij}^{L} = W_{ij}^{L} - l_r \cdot \sum_t \frac{\partial L_p}{\partial W_{ij}^{T,L}} \qquad (4)$$

This error rate is minimized during the training process by gradient descent and using equation 4, the latent weight is modified.

where is learning rate. $\sum_t \frac{\partial L_p}{\partial W_{ij}^{T,L}}$ is the total gradient in all time steps. However, gradient descent faces a degradation issue as the network depth increases [25]. In order to solve the degradation issue and to improve the training stability, in this manuscript, agnostic meta learning training [26] of the batch size of sampled task is considered W_{ij}^{L} in and loss as defined in equation 5.

$$l_f^{META}(\mu_0 \cdot \beta_0) = \sum_{w=1}^{W_{ij}^L} l_{fw}\left(U_i^{T,L}(\mu_0 \cdot \beta_0)\right) \tag{5}$$

μₒ, βₒ is the initial scaling and shifting parameters. These parameters obtain cross-task knowledge through agnostic meta-learning. The scaling and shifting parameters are updated for solving the problem of degradation and improving training stability according to the equation 6.

$$\mu_0 \cdot \beta_0 = (\mu_0 \cdot \beta_0) - \alpha \nabla_{\mu_0 \cdot \beta_0} \sum_{w=1}^{W_{ij}^L} l_{fw}\left(U_i^{T,L}(\mu_0 \cdot \beta_0)\right) \tag{6}$$

where, α is the learning rate used to improve the training stability. In order to perform further improvement in classification process, the weight parameter is optimized using improved billiards optimization algorithm.

D. Improved Billiards Optimization Algorithm

A wide range of metaheuristic optimizations have been created to provide the best solutions as a result of the complicated structure of current networks. The widely played game of pool had an impact on the Improved Billiards Optimization (IBO) approach [27]. In this research manuscript, the IBO algorithm is introduced for optimizing the weight, loss function, learning rate, scaling and shifting parameter to further improve the classification of attack and non-attack data.

The variables of ASBNN is initialized as in equation 7.

$$B_{n\cdot m}^{0} = V_m^{MIN} + r\left(V_m^{MAX} - V_m^{MIN}\right), n = 1.2.3...2N \text{ and } m = 1.2.3...M \tag{7}$$

where r is a random value in the range of 0 and 1, M and $2N$ represents the variable populations.

$$F_{func} = optimize\left\{W_{ij}^{L}, l_f, \mu, \beta\right\} \tag{8}$$

The fitness function is designed in equation 8 by identifying the placements of the ball and pocket.

Following the assessment of the pockets, balls are categorized according by fitness before being split into two equal groups, namely normal $(n = 1,...,N)$ and cue balls $(n = N+1,...,2N)$.

Pocket is selected by the following probability in equation 9 as follows,

$$p_c = \frac{e^{-\omega f_c}}{\sum_k e^{-\omega f_c}} \quad ; c = 1,2,...C \tag{9}$$

where, f_c is the objective function of c^{th} the pocket. ω is the pressure greater than 0.

In the surrounding of their pockets after collision, the current positions of regular balls are obtained. For improving the exploitation ability for optimizing $W_{ij}^{L}, l_f, \mu, \beta$ parameters, the search process is defined as follows. The current locations of normal balls are determined in equation 10 as

$$B_{N,M}^{new} = r_{[-E,E]}(1-R)\left(B_{N,M}^{old} - P_{C,M}^{N}\right) + P_{C,M}^{N} \tag{10}$$

$$, n = 1,2,3...N$$

where, $B_{N,M}^{new}$ and $B_{N,M}^{old}$ are the new and old M^{th} variable values from the n^{th} regular ball, R is the ratio of current iteration to maximum iterations. r is a random value and is the error rate. After updating new positions, the searching process is terminated if the criterion is satisfied by optimizing the parameters of ASBNN. Thus, the data detected as attack and non-attack data.

After classification, the non-attack data is transformed securely to the user in the upcoming section.

E. Secure Data Transmission

The non-attack data is secured using LW-PWECC framework which enhances privacy [28]. An light weight elliptic curve *E* is determined with the domain factors (m, n, k, R, l, s) over the prime field *F*ₖ. *R*is considered as the generator point.

By multiplying *R* by some integer between 0 and ϰ it generates other point in its sub group over the elliptic curve. In this cryptographic framework, the cryptographic strength is improved by ensuring large key space and resolving weak bit problem by choosing ϰ as infinity i.e. *R* is multiplied with some integers between zero and infinity to get all the subgroup points. There are several generator points in the elliptic curve. For choosing the best generator point and to reduce the overall computation period, a hybrid puzzle war optimization algorithm is used [29, 30]. The stepwise procedure of hybrid POA and WSA is depicted in Table 3.

TABLE 3: STEP WISE PROCEDURE OF HYBRID PUZZLE WAR OPTIMIZATION ALGORITHM

Input: Generator points in LW-PWECC **Output: Best generator points**
Begin *Define fitness function* $f(x) = select\ \{best\ R\}$

```
Define the POA parameters
Initialize the population as
$P = \begin{bmatrix} p_{1,1} & \cdots & p_{1,d} & \cdots & p_{1,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ p_{i,1} & \cdots & p_{i,d} & \cdots & p_{i,m} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ p_{N,1} & \cdots & p_{N,d} & \cdots & p_{N,m} \end{bmatrix}_{N\times m}$
while $(i < \max iterations)$
while $(i <= total variables)$
Choose a value from POA for the variable $d$
end if
else Choose a random number
end if
Determine the best solution using $O = P_k, R_i$
end while
Accept the new puzzle (solution) is better
end while
Find the current optimal solution
End
The optimal solution found by POA is considered as initial for WSO
while $(i < \max generation)$
Determine $\rho = rand$
Set a value for $\rho_r$
if $\rho < \rho_r$
Do Position updating
$P_i(t+1) = P_i(t) + 2\times\rho\times(K - P_{rand}(t)) + rand\times(W_i\times(C - P_i(t))$
else
Do Position updating
$P_i(t+1) = P_i(t) + 2\times\rho\times(C - K) + rand\times(W_i\times K - P_i(t))$
end if
Evaluate new solutions
If new solutions are better, update them in the population
end for
Find the current optimal solution $R_{best}$
end while
End
```

The selected generator points are given to the cryptographic encryption process. Equation 11 represents the elliptic curve.

$$Y^2 = X^3 + mX + n(\mathrm{mod}\ k) \tag{11}$$

$$A=c.K \quad where\ K,A\ Ɛ\ E(F_k) \tag{12}$$

An elliptic curve E with a fixed range F_k serves as the specification for the Elliptic Curve Discrete Logarithmic Problem (ECDLP). The points on the Elliptic Curve Cryptography (ECC) is described as K and L. Where, K takes the prime order l such that $A= d_{lt}.K$. d_{lt} is the discrete logarithmic task which determines the problem A.

Initialization

These parameters are generated and it selects the private key d_{lta} and estimates the public key which is defined in equation 13.

$$K_a = d_{lta}.\ R_{best} \tag{13}$$

Data Encryption

For encryption, a random value is chosen as an entity R_e over the main range F_k. The data D is encrypted using the below equation 14.

$$D_{enc} = D + K_m \cdot R_{best} \tag{14}$$

If an attacker gain access to this encrypted data, the private key is hidden from the attacker, therefore the original data is not changed.

Data Decryption

The encrypted data is decrypted using the below equation 15.

$$D' = D_{dec}, K_{m\cdot dec} \tag{15}$$

The proposed flow of secure data transmission is mentioned in the below Figure 4.

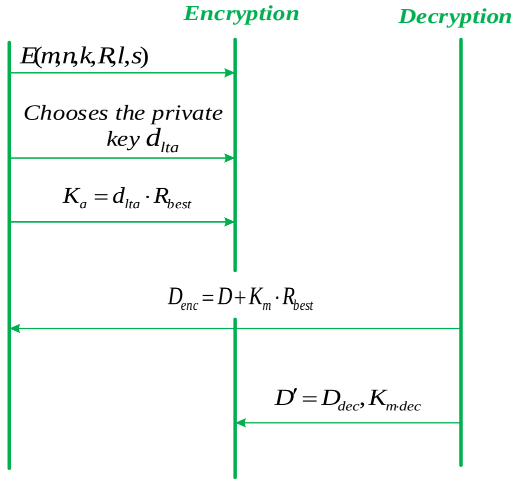
Encryption
Decryption
$E(m,n,k,R,l,s)$
Chooses the private key d_{lta}
$K_a = d_{lta}\cdot R_{best}$
$D_{enc} = D + K_m \cdot R_{best}$
$D' = D_{dec}, K_{m\cdot dec}$

Figure 4: Encryption and Decryption process

After encryption and decryption, the decrypted data is exhibited on the IoT device. Thus, the proposed detection technique ASB-IB detects the attacks accurately with improved stability by solving the degradation issue and the proposed cryptographic framework transmits the data securely with high security and minimal error rate.

4. OUTCOME OF INTRODUCED MODEL

The results of the proposed ASB-IB and LW-PWECC methods are implemented using MATLAB. Several existing classifiers like Dual CNN [15], LSTM, Spiking Neural Network (SNN), Binarized Spiking Neural Network (BSNN) [17, 31] and encryption methods like Identity-Based Encryption (IBE) [32], Advanced Encryption Standard (AES) [33], Rivest-Shamir-Adleman (RSA) [34] and ECC [35] are taken to compare the performance of the introduced approach.

A. Statistical analyses

The McNeymars test of statistics was computed by continuous correction. The critical value at 95% significance level was 3.8415. McNeymar chi-squared coefficient (with Yates'es correction) is 20.672222 and the probability value, (p)is0.000005.

The Wilcoxon rank test was computed for comparing the independent attack and non-attack data. The p value is obtained as 0.0043.

From this result, it is noted that the proposed technique is statistically significant as the probability (p) value is very lesser than 0.05.

B. Evaluation matrices

The performance evaluation is done using various matrices like precision, sensitivity, f-score, specificity, accuracy, cumulative accuracy, computational time, encryption time, decryption time, security level and delay. Table 4 depicts the evaluation parameters.

TABLE 4: EVALUATION PARAMETERS

Outcome	*Symbol*	*Description*
True Positive	T_P	Correctly detected as attack data
True Negative	T_N	Correctly detected as non-attack data
False Positive	F_P	Incorrectly detected as attack data
False Negative	F_N	Incorrectly detected as non-attack data

C. Performance evaluation

In this section, the performance evaluation of the introduced technique is done with several classifiers and encryption techniques.

Figure 5 explains the several attacks and non-attack data using the introduced technique. The attacks are accurately detected as DoS attack, ARP spoofing, NMAP port scan, Smurf attack and non-attack.

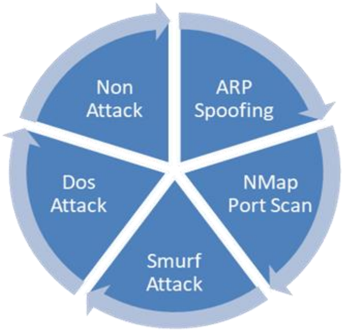

Figure 5: Rate of attack detection

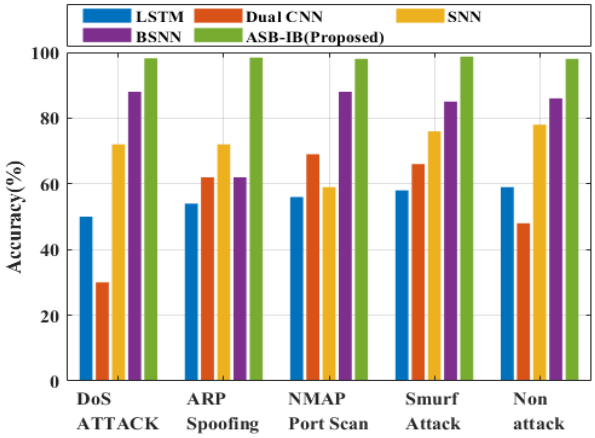

Figure 6(a): Comparison of Accuracy %

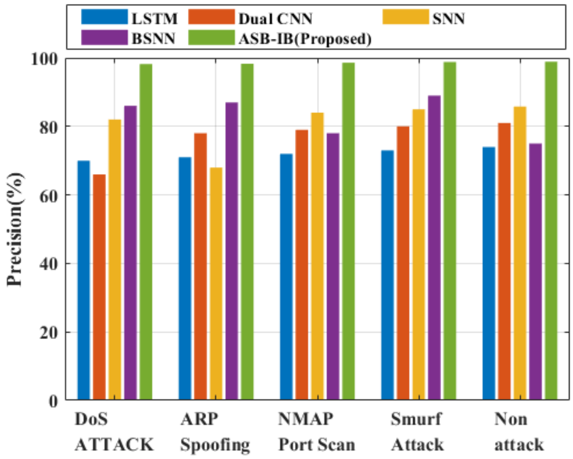

Figure 6(b): Comparison of Precision %

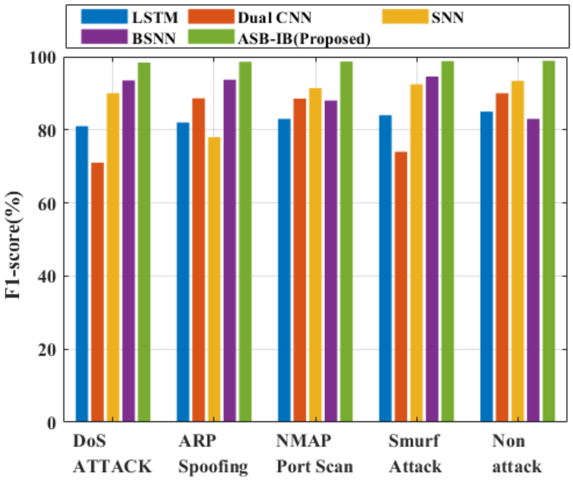

Figure 6(c): Comparison of F1 score %

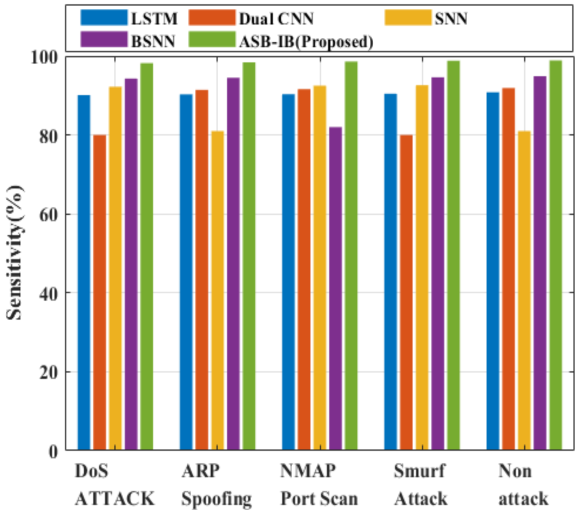

Figure 6(d): Comparison of Sensitivity %

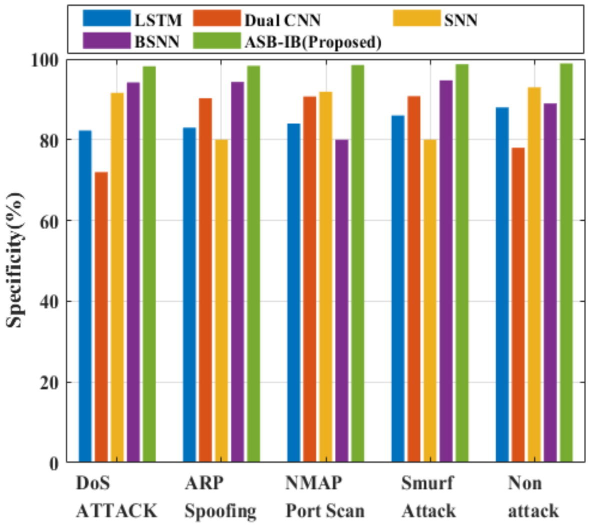

Figure 6(e): Comparison of Specificity %

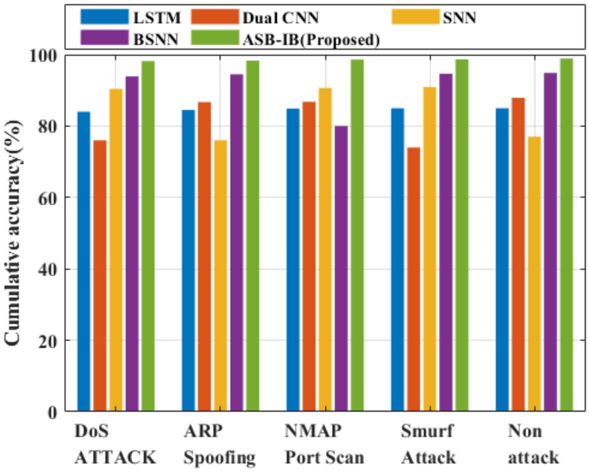

Figure 6(f): Comparison of cumulative accuracy score %

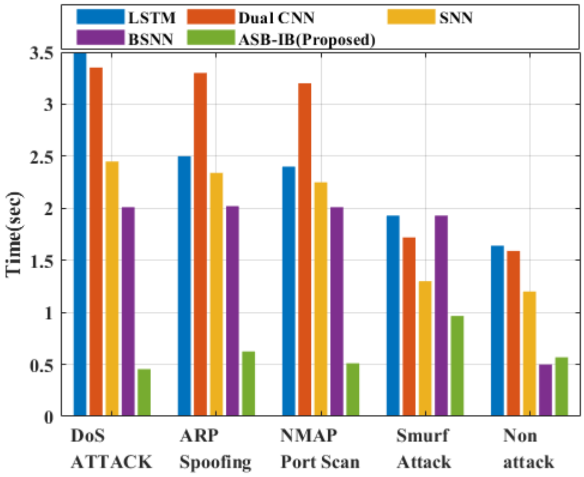

Figure 6(f): Comparison of time (sec)

Figure 6(a-g) briefly explains the evaluation of the introduced classifier ASB-IB with other classifiers such as LSTM, CNN, SNN and BSNN in various stages of attack and non-attack. BSNN is updated as ASB-IB with the hybrid of improved billiards algorithm with ASB. The agnostic learning in the introduced model paves the way for improving the training stability of the proposed method by solving the degradation problem. Because of good training stability, ASB-IB performs better in terms of precision, F1-score, specificity, computational time, cumulative accuracy, accuracy and sensitivity.

In Figure 7, the proposed encryption and decryption model is compared and analyzed with other existing encryption technique in case of secure data transmission. The major problem in the existing approaches like high delay and insecurity are overcame as shown in the above Figure 7(c) and 7(d) by integrating light weight cryptography with puzzle war elliptic curve cryptography.

Because it uses less memory, limited computational resources and a less amount of power for transmission of data securely. The encryption and decryption time are also compared as shown in Figure 7(a) and 7(b) and proven that LW-PWECC achieved a lower period of time for the process than the traditional approaches.

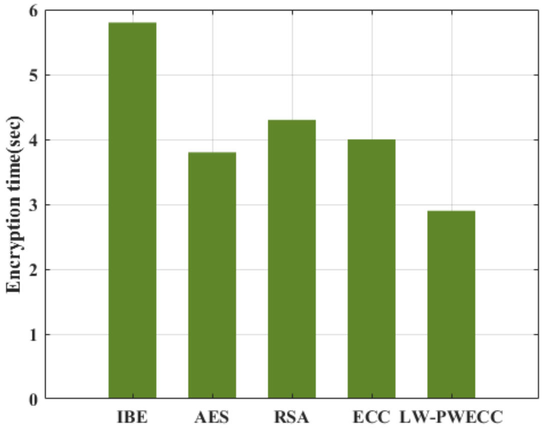

Figure 7(a): Comparison of encryption time (sec)

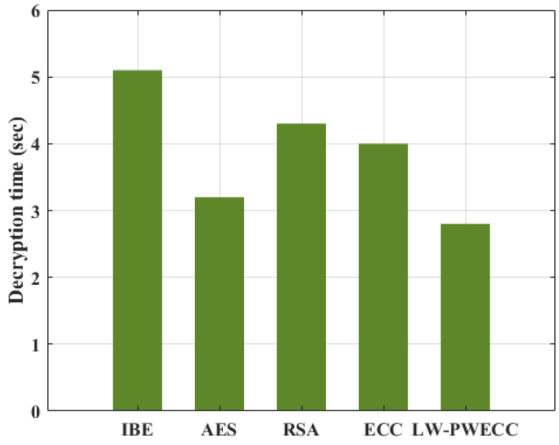

Figure 7(b): Comparison of decryption time (sec)

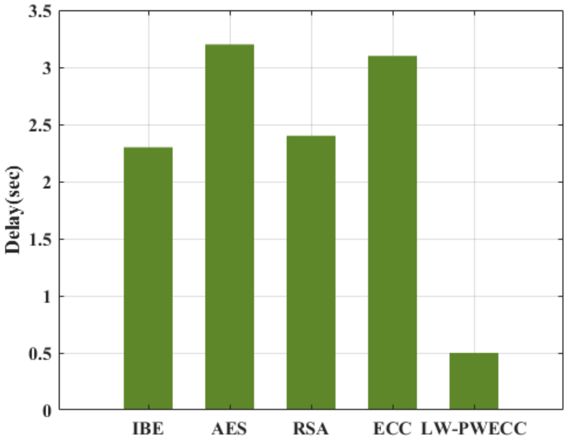

Figure 7(c): Comparison of delay time (sec)

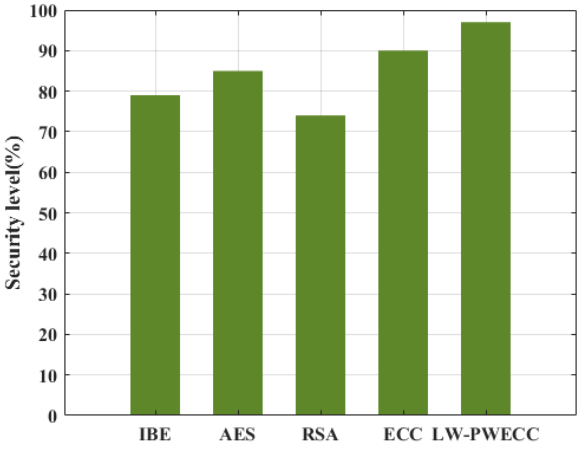

Figure 7(d): Comparison of security level (sec)

The accuracy and loss curve with the number of iterations is depicted in Figure 8(a) and 8(b). The accuracy curve in Figure 8(a) is depicted for about 300 iterations shows that the accuracy of training and testing is more identical and increases with increase in epochs and maintains a constant value after 100 epochs. Hence, it is demonstrated that the new technique does not overfit the training set of data and provides a decent generalization for previously unknown data. The loss curve in Figure 8(b) decreases with increase in epochs. The testing loss is slightly higher for about 100 epochs and after that testing loss falls.

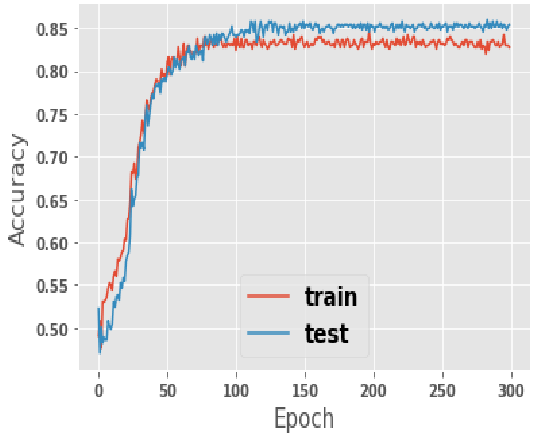

Figure 8(a): Accuracy v/s Epoch

Figure 9 shows the overall detection rate of several attacks like DoS, ARP Spoofing, NMAP Port Scan, Smurf Attack and non-attack (normal) data by using ASB-IB. Table 5 represents the comparison of overall accuracy, precision, recall, F1-score, training time and execution time using the ECU-IoHT dataset. The other traditional approaches used for comparing the overall accuracy such as DNN [18], MSCSL [20] also uses the ECU-IoHT dataset for attack detection and data security.

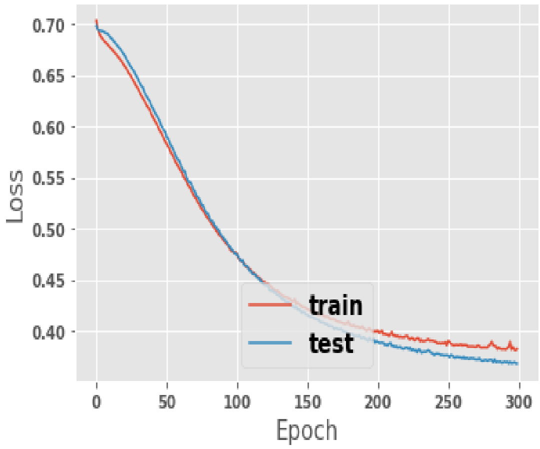

Figure 8(b): Loss v/s Epoch

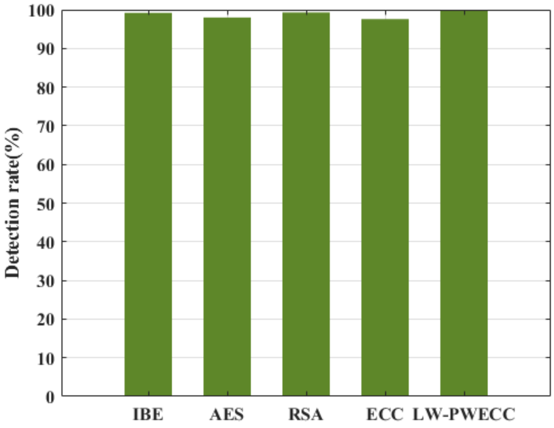

Figure 9: Detection Rate

This model achieves an accuracy of 99.99% which is comparatively higher than existing models because of updating the learning rate, weight, loss function, scaling and shifting parameter of agnostic binarized spiking neural network with the improved billiards optimization algorithm. Also, the novel cryptographic framework proves the effectiveness of the proposed model with limited computational resources and this model reduces the execution time of the overall process by integration with hybrid optimization algorithms.

5. CONCLUSION

The ASB-IB for accurate detection of network attacks and LW-PWECC framework for secure data transmission is successfully implemented using MATLAB. The training stability which is considered as the major problem is improved by performing an agnostic meta learning training of binarized spiking neural network by solving the degradation issue. Maximum accuracy of detection, high security and minimal delay of transmitting the non-attack data is achieved by updating the learning rate, weight, loss function, scaling and shifting parameter of agnostic binarized spiking neural network with the improved billiards optimization algorithm. Compared with the traditional techniques, the introduced approach achieved an overall higher accuracy of 99.99%, overall lower training time of 0.028 secs with high security and minimal delay. The analyses on Mc Neymar and Wilcoxon Rank Sum tests shows that the introduced model is statistically significant. The future work of the suggested approach will be done by deploying the framework in the cloud infrastructure.

ACKNOWLEDGMENT

The completion of this research would not have been possible without the contributions and support of many individuals and organizations. Our gratitude for Dr Shashidahara H R, Dr Abhilash C N and Chetan R. In addition, we would like to extend our sincere thanks to all of the participants in our study, who generously shared their time, experiences, and insights with us.

REFERENCES

[1] Qureshi, KashifNaseer, Shahid Saeed Rana, Awais Ahmed, and Gwanggil Jeon. "A novel and secure attacks detection framework for smart cities industrial internet of things." Sustainable Cities and Society 61 (2020): 102343.

[2] Lima Filho FS, Silveira FA, de Medeiros Brito Junior A, Vargas-Solar G, Silveira LF. Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks. 2019 Oct 13;2019: 1-5.

[3] Velayudhan, Nitha C., A. Anitha, and MukeshMadanan. "Sybil attack detection and secure data transmission in VANET using CMEHA-DNN and MD5-ECC." Journal of Ambient Intelligence and Humanized Computing (2021): 1-13.

[4] Anand, C., and N. Vasuki. "Trust based DoS attack detection in wireless sensor networks for reliable data transmission." Wireless Personal Communications 121, no. 4 (2021): 2911-2926.

[5] Alzubi, Jafar A. "Bipolar fully recurrent deep structured neural learning-based attack detection for securing industrial sensor networks." Transactions on Emerging Telecommunications Technologies 32, no. 7 (2021): e4069.

[6] Tekerek, Adem. "A novel architecture for web-based attack detection using convolutional neural network." Computers & Security 100 (2021): 102096.

[7] Diro, Abebe, and Naveen Chilamkurti. "Leveraging LSTM networks for attack detection in fog-to-things communications." IEEE Communications Magazine 56, no. 9 (2018): 124-130.

[8] Alsamiri, Jadel, and Khalid Alsubhi. "Internet of things cyberattacks detection using machine learning." International Journal of Advanced Computer Science and Applications 10, no. 12 (2019).

[9] Syed, NaeemFirdous, ZubairBaig, Ahmed Ibrahim, and Craig Valli. "Denial of service attack detection through machine learning for the IoT." Journal of Information and Telecommunication 4, no. 4 (2020): 482-503.

[10] Gu, Tianbo, Allaukik Abhishek, Hao Fu, Huanle Zhang, DebrajBasu, and PrasantMohapatra. "Towards learning-automation IoT attack detection through reinforcement learning." In 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), pp. 88-97. IEEE, 2020.

[11] Justindhas, Y., and P. Jeyanthi. "Attack detection and prevention in IoT-SCADA networks using NK-classifier." Soft Computing 26, no. 14 (2022): 6811-6823.

[12] Aouedi, Ons, KandarajPiamrat, Guillaume Muller, and Kamal Singh. "Federated semisupervised learning for attack detection in industrial Internet of Things." IEEE Transactions on Industrial Informatics 19, no. 1 (2022): 286-295.

[13] Gudla, Surya Pavan Kumar, Sourav Kumar Bhoi, SoumyaRanjanNayak, and Amit Verma. "DI-ADS: a deep intelligent distributed denial of service attack detection scheme for fog-based IoT applications." Mathematical Problems in Engineering 2022 (2022): 1-17.

[14] Duraisamy, A., Subramaniam, M. Attack Detection on IoT Based Smart Cities using IDS Based MANFIS Classifier and Secure Data Transmission Using IRSA Encryption. Wireless PersCommun 119, 1913–1934 (2021).

[15] Alabsi BA, Anbar M, Rihan SD. CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks. Sensors. 2023 Jul 19;23(14):6507.

[16] Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, AlirezaJolfaei, and AKM Najmul Islam. "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system." Journal of Parallel and Distributed Computing 172 (2023): 69-83.

[17] Priyadarshini I, Mohanty P, Alkhayyat A, Sharma R, Kumar S. SDN and application layer DDoS attacks detection in IoT devices by attention ‐ based Bi ‐ LSTM ‐ CNN. Transactions on Emerging Telecommunications Technologies. 2023 Mar 14: e4758.

[18] Vijayakumar KP, Pradeep K, Balasundaram A, Prusty MR. Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network. Processes. 2023 Apr 3;11(4):1072.

[19] Ezhilarasi M, Gnanaprasanambikai L, Kousalya A, Shanmugapriya M. A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. Soft Computing. 2023 Apr;27(7):4157-68.

[20] Thulasi T, Sivamohan K. LSO-CSL: Light spectrum optimizer-based convolutional stacked long short-term memory for attack detection in IoT-based healthcare applications. Expert Systems with Applications. 2023 Dec 1;232: 120772.

[21] Sankaran KS, Kim BH. Deep learning-based energy efficient optimal RMC-CNN model for secured data transmission and anomaly detection in industrial IOT. Sustainable Energy Technologies and Assessments. 2023 Mar 1;56: 102983.

[22] https://ro.ecu.edu.au/datasets/48/

[23] Duraisamy, Ayyer, Muthusamy Subramaniam, and Chinnanadar Ramachandran RENE Robin. "An optimized deep learning-based security enhancement and attack detection on IoT using IDS and KH-AES for smart cities." Studies in Informatics and Control 30, no. 2 (2021): 121-131.

[24] Hosseini, Eghbal, Ali SafaaSadiq, KayhanZrarGhafoor, Danda B. Rawat, MehrdadSaif, and Xinan Yang. "Volcano eruption algorithm for solving optimization problems." Neural Computing and Applications 33 (2021): 2321-2337.

[25] Nguyen, Van-Tinh, Quang-Kien Trinh, Renyuan Zhang, and Yasuhiko Nakashima. "STT-BSNN: an in-memory deep binary spiking neural network based on STT-MRAM." IEEE Access 9 (2021): 151373-151385.

[26] Yao, Xiao, Jianlong Zhu, GuanyingHuo, Ning Xu, Xiaofeng Liu, and Ce Zhang. "Model-agnostic multi-stage loss optimization meta learning." International Journal of Machine Learning and Cybernetics 12, no. 8 (2021): 2349-2363.

[27] Kaveh, A., M. Khanzadi, and M. RastegarMoghaddam. "Billiards-inspired optimization algorithm; a new meta-heuristic method." In Structures, vol. 27, pp. 1722-1739. Elsevier, 2020.

[28] Justindhas, Y., and P. Jeyanthi. "Attack detection and prevention in IoT-SCADA networks using NK-classifier." Soft Computing 26, no. 14 (2022): 6811-6823.

[29] Ayyarao, Tummala SLV, N. S. S. Ramakrishna, Rajvikram Madurai Elavarasan, Nishanth Polumahanthi, M. Rambabu, Gaurav Saini, Baseem Khan, and Bilal Alatas. "War strategy optimization algorithm: a new effective metaheuristic algorithm for global optimization." IEEE Access 10 (2022): 25073-25105.

[30] Zeidabadi, Fatemeh Ahmadi, and Mohammad Dehghani. "POA: Puzzle optimization algorithm." Int. J. Intell. Eng. Syst 15, no. 1 (2022): 273-281.

[31] Liang, Ling, Xing Hu, Lei Deng, Yujie Wu, Guoqi Li, Yufei Ding, Peng Li, and Yuan Xie. "Exploring adversarial attack in spiking neural networks with spike-compatible gradient." IEEE transactions on neural networks and learning systems (2021).

[32] Bhandari, Rupesh, and V. B. Kirubanand. "Enhanced encryption technique for secure iot data transmission." International Journal of Electrical and Computer Engineering 9, no. 5 (2019): 3732.

[33] Ahmed, Mohammed Altaf, and SulemanAlnatheer. "Deep Q-Learning with Bit-Swapping-Based Linear Feedback Shift Register fostered Built-In Self-Test and Built-In Self-Repair for SRAM." Micromachines 13, no. 6 (2022): 971.

[34] Rathore, Shailendra, and Jong Hyuk Park. "Semi-supervised learning based distributed attack detection framework for IoT." Applied Soft Computing 72 (2018): 79-89.

[35] Majumder, Suman, Sangram Ray, DipanwitaSadhukhan, Muhammad Khurram Khan, and MouDasgupta. "ECC-CoAP: Elliptic curve cryptography-based constraint application protocol for internet of things." Wireless Personal Communications 116 (2021): 1867-1896.