Journal of Robotics and Control (JRC)
Volume 5, Issue 1, 2024
ISSN: 2715-5072, DOI: 10.18196/jrc.v5i1.20514

LW-PWECC: Cryptographic Framework of Attack Detection and Secure Data Transmission in IoT

Ranjith J [1*], Mahantesh K [2], Abhilash C N [3]
[1, 3] Department of Information Science and Engineering, SJB Institute of Technology, Bengaluru, India
[2] Department of Electronics and Communication Engineering, SJB Institute of Technology, Bengaluru, India
Email: [1] ranjithj@sjbit.edu.in, [2] kmahantesh@sjbit.edu.in, [3] cnabhilash@sjbit.edu.in
*Corresponding Author

***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 existing however 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 99.93% 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.

I. 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]. 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].

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]. devices transmit and receive data wirelessly, which increases the possibility of wireless sensor network (WSN) security breaches in IoHT [11]. Furthermore, the Internet is the main source of security risks and is open to several types of cyberattacks, including denial-of-service attacks [12]. In IoHT situations, network spying, medical record theft [13], and therapy modification are all possible. Cybersecurity is essential for defending networks and data against many types of cyberattacks. As such, developing a method for identifying different kinds of IoHT attacks is crucial. In addition to the safety concerns, the datasets linked to the cyberattacks are not publicly accessible in the medical profession since they put sensitive patient data at risk, which could cause harm or even result in patient death [14]. To mitigate the aforementioned dangers, we employ the innovative ECU-IoHT dataset [15], which represents a range of cyber-attacks. Identified Security Attributes (ISA) for applying multi-criteria decision-making (MCDM) techniques to assess the security aspects of Internet of Health Things (IoHT) systems. By identifying and assessing security requirements, the framework seeks to address the security risks of IoHT devices in healthcare settings [16]. Because gait analysis and chronic diseases are closely related, it is significant in the healthcare industry. The emergence of the Internet of Health Things (IoHT) has made it possible to remotely monitor and analyse gait over an extended period of time, saving patients' time and money on transportation while giving physicians access to more useful gait data [17]. Internet of Health Things (IoHT) networks has privacy requirements within a healthcare

setting. However, these networks have unique challenges and security requirements (integrity, authentication, privacy and availability) must also be balanced with the need to maintain efficiency in order to conserve battery power, which can be a significant limitation in IoHT devices and networks [18]. Internet of Medical Things (IoMT)-based blockchain-assisted secure data management architecture for health information analysis. The framework tackles the issues of data accessibility, scalability, privacy, and security in the IoMT. It makes use of blockchain technology to improve scalability and data accessibility in the healthcare setting while facilitating the safe transmission of patient data [19]. federated learning offers clear privacy benefits over data canter training in terms of safeguarding private information [20].

The research contributions of this paper are as follows:

- A novel deep learning technique called Agnostic Spiking Binarized neural network with Improved Billiards optimization (ASB-IB) for accurate detection of network attacks and Light Weight integrated Puzzle War Elliptic Curve Cryptographic (LW-PWECC) framework for secure data transmission with high security and minimal delay is proposed.
- By performing an agnostic meta learning training of binarized spiking neural network, this method solves the degradation issue and improves the training stability.
- By optimizing the learning rate, weight, loss function, scaling and shifting parameter of agnostic binarized spiking neural network with the improved billiards optimization algorithm, the introduced model achieves maximum accuracy of detection, high security and minimal delay of transmitting the non-attack data.
- In the cryptographic framework, the best generator points of the elliptic curve are selected by the hybrid of Puzzle Optimization Algorithm (POA) and War Strategy Algorithm (WSA).
- The Mc-Neymar and Wilcoxon Rank Sum test are done and proves that the introduced model is statistically significant.

The following sections of this paper are structured as follows: section 2 introduces briefly methods proposed and backgrounds and presents the proposed method; section 3 gives the results and discussions brief about accuracy of the proposed method. In section 4 conclusion and future works are discussed.

II. METHODS AND BACKGROUND

To carryout research on challenges in IoTH various articles is studied and made a summary to include in background work.

Among the many obstacles to the implementation of next-generation mH-IoT, particularly in COVID-19 outbreaks, are data availability and dependability. Thus, to combat such pandemics, stronger and more intelligent health care frameworks are needed. Reinforcement learning (RL) has demonstrated its capacity to deliver intelligent data availability and reliability in recent times [21]. Such sensor networks can be made secure with the help of asymmetric cryptography techniques. The safe CoAP is compatible with the Datagram Transport Layer Security (DTLS) protocol for establishing a secure session utilizing pre-existing techniques like Lightweight Establishment of Secure Session [22] for communication between various IoMT devices and a remote server. A thorough and organized PHM framework is lacking in order to produce greater added value [23]. Safe biomedical picture transfer and retrieval across Internet of Things networks. In order to do this, the biological pictures are encrypted using the five-dimensional hyper-chaotic map (FDHC) and compressive sensing [24].

It is imperative that Indonesia develop a strategy for telehealth systems in light of the growing use of information technology in the healthcare industry [25]. The connected health paradigm is now widely accepted because to the Internet of Health Things (IoHT). IoHT is able to provide linked health monitoring with ultra-low latency and high quality of service thanks to 5G support in the healthcare vertical. Deep learning has demonstrated promise in automating linked healthcare workflows, processing enormous amounts of IoHT data created every day, and supporting decision-making processes [26]. A collaborative edge-fog-cloud healthcare framework on the go. It makes use of cloud-based health data analysis in the event of anomalous health status, as well as edge and fog sensors for customizable health monitoring. Users' constant changing of locations is a serious problem, and in an emergency, a lost connection and a delay in the delivery of health-related data could be fatal [27]. IoHT primarily addresses the wireless connectivity of the body sensor and medical device networks to the cloud, enabling the gathering, sorting, and processing of health data. Real-time data collection health devices follow the right protocols for secure connections and effective machine-to-machine data transfer [28].

A single, integrated computer framework for real-time smart healthcare domains that combines several computing techniques. Then provide recommendations for the best network infrastructure deployment based on hospital scale-patients, taking into account the effectiveness of the suggested solution using the queue network model tool [29]. KREATION is a Kotlin framework for creating IoHT apps for Android smartphones that are self-adaptive. The Model-View-Control architecture was utilized in the development of this framework, which integrates the MAPE-K adaption loop into its internal logic. Additionally, it provides methods for gathering information from the sensors of Android smartphones and the Google Fit API, which enables you to access information gathered from additional Android devices, like smartwatches and bands [30].

The providing of secured services continues to be a significant difficulty in spite of significant efforts made in this regard. In order to encourage further research in this field, this work offers a thorough description of the present difficulties and solutions for delivering secured service provisioning, with a focus on IoHT assaults and counter measures [31]. IoT-driven healthcare models can help physicians give better treatment by keeping patients safe and well. Furthermore, healthcare frameworks enhance

performance and drastically save healthcare expenses. Because blockchain systems are transparent, sharing and storing private data on them is secure. As part of the proposed architecture, medical device data is stored on a cloud server along with pertinent medical reports [32].

Numerous sensors, controllers, and actuators enable the integration, calculation, and interoperability. One of the key elements for the devices' communication to function properly and carry out healthcare operations is security [33]. Digital photographs are a way to electronically convey patient information that is sensitive in the healthcare area. To ensure the privacy of these pictures, a robust and quick cryptosystem must be designed. The plan uses a Piecewise Linear Chaotic Map (PWLCM), a Chebyshev map, and a logistic map to disperse and confuse the medical image [34]. The Internet of Health Things (IoHT) has steadily advanced and improved throughout time. Higher Quality of Service (QoS) is thought to be a significant problem when creating such systems to provide faster replies and data-specific sophisticated analytics services, though, due to the unstructured and crucial nature of healthcare data [35].

To create a safe environment, Internet of Healthcare Things (IoHT) devices need to be secured by strong intrusion detection systems (IDS). In order to protect users' privacy, federated learning has drawn interest from the government and healthcare institutions as it is unpleasant to gather this data and carry out machine learning tasks directly [36]. Patient parameters can be instantly deployed to the cloud and monitored. A Raspberry Pi 4B System-on-a-Chip (SoC) computer is used in the construction of the suggested IoHT framework. The measured values of bodily parameters, such as temperature, heart rate, and SpO2 levels, provide the foundation for medical treatment [37]. Various countries and businesses have provided security regulations and guidelines to characterize the recommended processes for the security of individual wellbeing in response to the growing number of occurrences of protection breaches on social insurance information [38]. By providing cloud-like processing and storage capabilities with a low latency and less bandwidth, fog computing's architecture and latency benefit mobile nodes and 5G IoHT devices. Fog computing is a method for offloading tasks from programs operating on edge devices as a result of this added behavior [39].

In this section, the proposed approach on accurate and efficient attack detection using ASB-IB and secure data transmission using LW-PWECCis explained in detail. Fig. 1 depicts the work flow of introduced technique.

The proposed deep learning strategy in this paper is evaluated using the ECU-IoHT [20] dataset in the health care area. There are 111,207 samples in the dataset, encompassing both common and uncommon assault types. Table I provides a full explanation of the amount of counts for normal and additional attack labels in the original dataset, including ARP spoofing, DoS attacks, Nmap PortScan, and Smurf attacks.

Preprocessing of the input, selecting optimal features using volcanic eruption optimization algorithm (VEO), IoT forecasting is done using light weight elliptical curve cryptography, attack detection using Agnostic Spiking Binarized Neural Network (ASB-IB) and transmission of data are the various stages of introduced method.

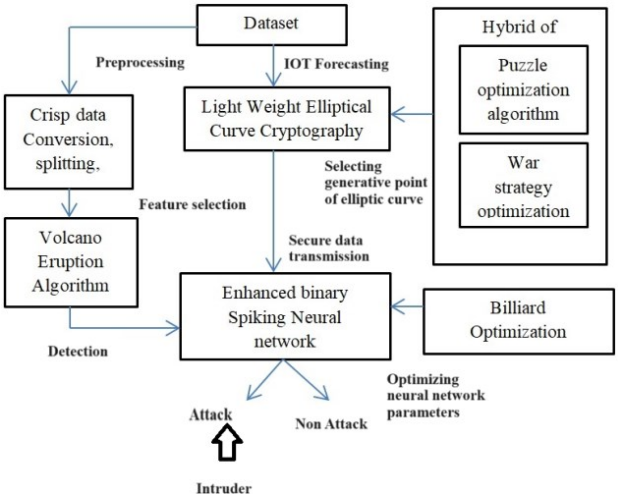


Fig. 1. Work flow of proposed approach

TABLE I. DESCRIPTION ABOUT ECU-IOHT DATA SET

Category	ECU-IoHT in Proposed work	
	Count	Training (35%)
Non Attack	23453	8206
ARP Spoofing	2359	826
DoS Attack	639	224
Nmap port scan	6836	2393
Smurf attack	77920	22272

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 [15]. The preprocessing of the IoHT data involves crisp data conversion, splitting and normalization [52].

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

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

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 [52]. The stepwise procedure of selecting best features for attack detection is given in Algorithm 1.

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

Algorithm 1 *Volcano Eruption Optimization*

Input: Preprocessed output
Output: Feature selection
Description:
1. Generate initial populations
2. n: number of solutions
3. p: given positive number
4. for$i = 1$to$n$do
5. Randomly generate solution of populations
6. C: random number
7. D_{rj}: j^{th}random direction
8. Calculate the fitness function
9. The solutions of current populations are exploded and erupted for selecting best features
10. 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 Fig. 2.

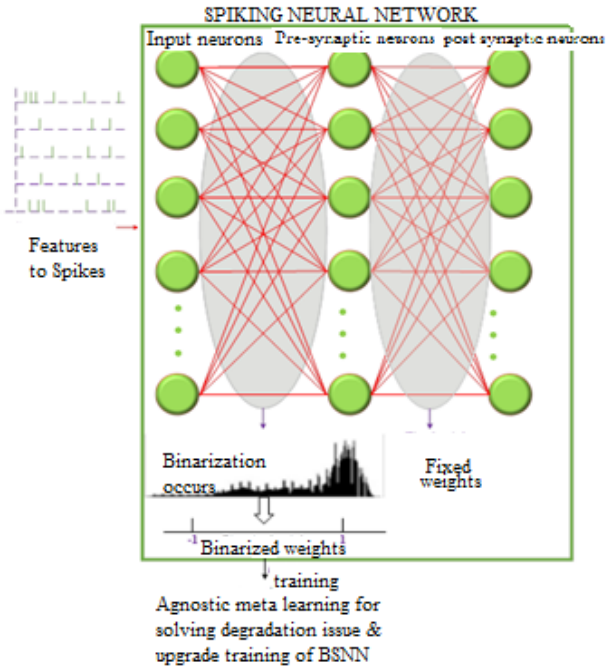


Fig. 2. Architecture of proposed neural network

In the training process, the binarized weights are signified in bipolar setup. The membrane potential $U_i^{T,L}$ f for i^{th} neuron at time step t in layer l is defined in equation (2).

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

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.

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.

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

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

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

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 [54]. 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).

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

μ_o, β_o 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).

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

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 [55]. 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 are initialized as in equation (7).

$$B_{n\cdot m}^{0} = V_m^{MIN} + r(V_m^{MAX} - V_m^{MIN}), n = 1.2.3\ldots 2N \; and \; m = 1.2.3\ldots M \quad (7)$$

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

$$F_{func} = optimize\{W_{ij}^{L}, l_f, \mu, \beta\} \quad (8)$$

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 $(n = 1,\ldots,N)$ and cue balls $(n = N+1,\ldots,2N)$. Pocket is selected by the following probability in equation (9) as follows,

$$p_c = \frac{e^{-\omega f_c}}{\sum_k e^{-\omega f_c}}; c = 1,2,\ldots C \quad ()$$

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

$$B_{N,M}^{new} = r_{[-E,E]}(1-R)\left(B_{N,M}^{old} - P_{C,M}^{N}\right) + P_{C,M}^{N}, n = 1,2,3\ldots N \quad (10)$$

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 [57]. 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 $\varkappa$ 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 $\varkappa$ 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 [58][59]. The stepwise procedure of hybrid POA and WSA is depicted in Algorithm 2 Optimization Algorithm.

Algorithm 2 Optimization Algorithm

Input: Generator points in LW-PWECC
Output: Best generator points
Description:

1. Begin
2. Define fitness function $f(x) = select\{bestR\}$
3. Define the POA parameters
4. Initialize the population as
$$P = \begin{bmatrix} p_{1,1} & \cdots & p_{1,d} & \cdots & p_{1,m} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ p_{i,1} & \cdots & p_{i,d} & \cdots & p_{i,m} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ p_{N,1} & \cdots & p_{N,d} & \cdots & p_{N,m} \end{bmatrix}_{N\times m}$$
5. while$(i < max\ iterations)$
6. while$(i <= totalvariables)$
7. Choose a value from POA for the variable d
8. end if
9. else Choose a random number
10. end if
11. Determine the best solution using $O = P_k, R_i$
12. end while
13. Accept the new puzzle (solution) is better
14. end while
15. Find the current optimal solution
16. End
17. The optimal solution found by POA is considered as initial for WSO
18. While $(i < max\ generation)$
19. Determine $\rho = rand$
20. Set a value for ρ_r
21. If $\rho < \rho_r$
22. Do Position updating
23. $P_i(t+1) = P_i(t) + 2 \times \rho \times (K - P_{rand}(t)) + rand \times (W_i \times (C - P_i(t))$
24. else
25. Do Position updating
26. $P_i(t+1) = P_i(t) + 2 \times \rho \times (C - K) + rand \times (W_i \times K - P_i(t))$
27. end if
28. Evaluate new solutions
29. If new solutions are better, update them in the population
30. end for
31. Find the current optimal solution Rbest
32. end while
33. End

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

$$Y^2 = X^3 + mX + n(mod\ k) \quad (11)$$

$$A = c.K \;\; where\ K, A\ \Sigma\ E(F_k) \quad (12)$$

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 $A = dlt.K$. dlt is the discrete logarithmic task which determines the problem A.

Initialization: These parameters are generated and it selects the private key dlta and estimates the public key which is defined in equation (13).

$$K_a = d_{lta}.R_{best} \quad (13)$$

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).

$$D_{enc} = D + K_m \cdot R_{best} \quad (14)$$

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).

$$D' = D_{dec}, K_{m \cdot dec} \quad (15)$$

The proposed flow of secure data transmission is mentioned in the below Fig. 3.

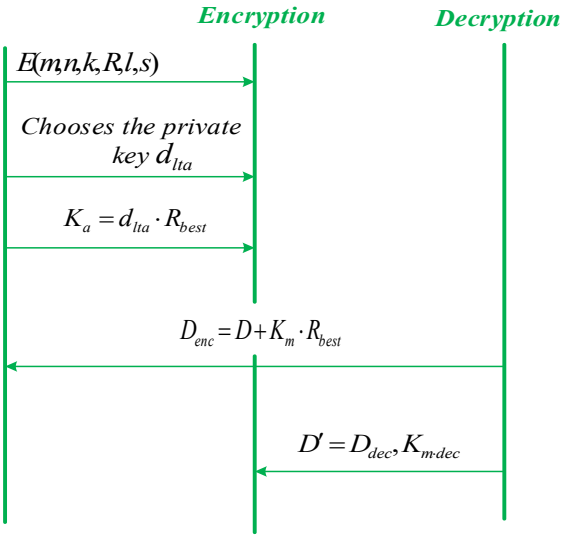


Fig. 3. Encryption and decryption process

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.

III. Results and Discussion

The results of the proposed ASB-IB and LW-PWECC methods are implemented. Several existing classifiers like Dual CNN [44], LSTM, Spiking Neural Network (SNN), Binarized Spiking Neural Network (BSNN) [46][59] and encryption methods like Identity-Based Encryption (IBE) [60], Advanced Encryption Standard (AES) [63], Rivest-Shamir-Adleman (RSA) [64] and ECC [63] are taken to compare the performance of the introduced approach.

The experimental setup of the proposed work is carried by contacting on environmental setup of lenova machine with installed with windows 10,16GB RAM , Intel i9 core processor 13900KF , PyDev IDE (version 10.2.0) with matplot libraries , Numpy (version 1.20),Tensor flow(version 3.7).

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) is 0.000005.

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 II depicts the evaluation parameters.

TABLE II. 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

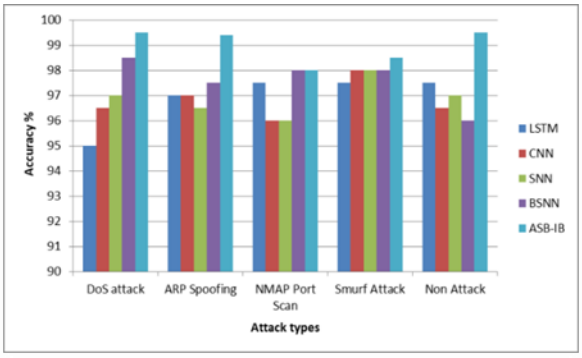
C. Performance Evaluation

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

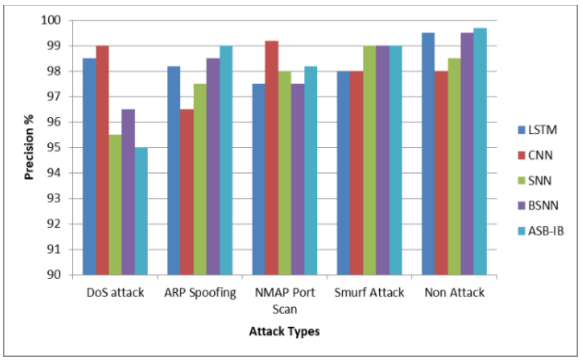
Fig. 4 explains the several attacks and non-attack data using the introduced technique. The attacks are accurately detected as DoS attack, ARP spoofing, NMAP port scan, Smurf attack and non-attack.

Fig. 4. Rate of attack detection

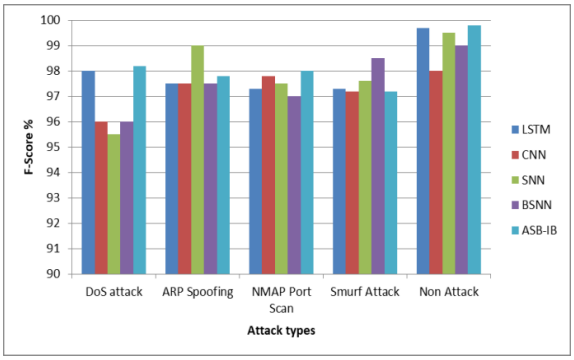
Fig. 5(a)-(g) briefly explains the evaluation of the introduced classifier ASB-IB with other classifiers such as LSTM, CNN, SNN and BSNN in various stages of attack and non-attack. BSNN is updated as ASB-IB with the hybrid of improved billiards algorithm with ASB. The agnostic learning in the introduced 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 Fig. 6, the proposed encryption and decryption model is compared and analyzed with other existing encryption technique in case of secure data transmission.



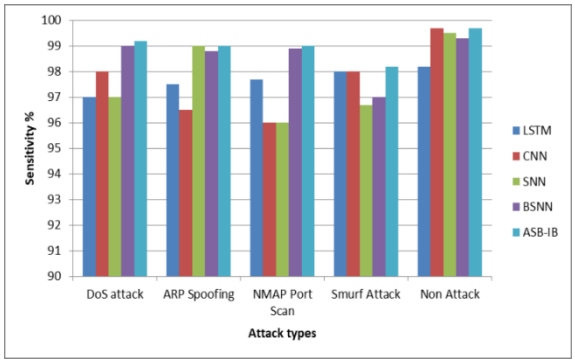
(a). Comparison of Accuracy %



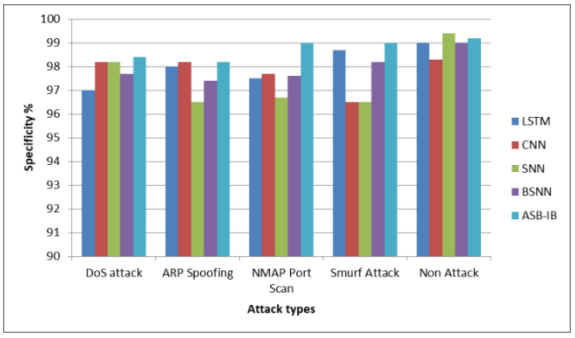
(b). Comparison of Precision %



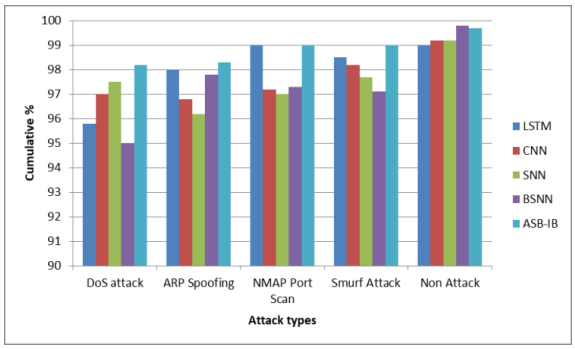
(c). Comparison of F1 score %



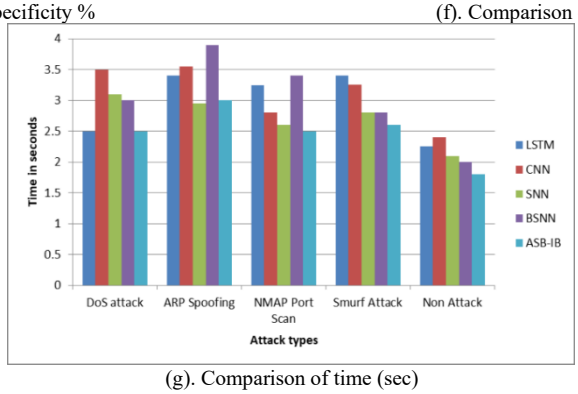
(d). Comparison of Sensitivity %



(e). Comparison of Specificity %

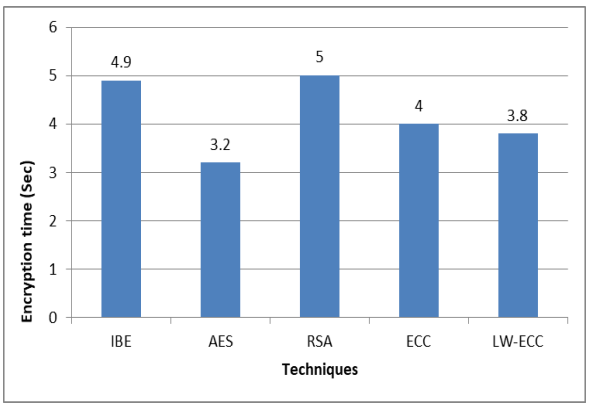


(f). Comparison of cumulative accuracy score %

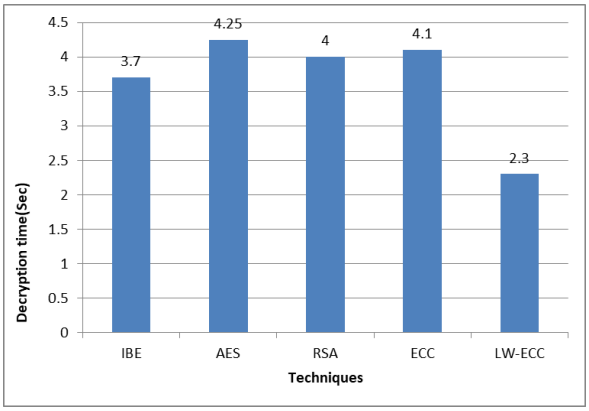


(g). Comparison of time (sec)

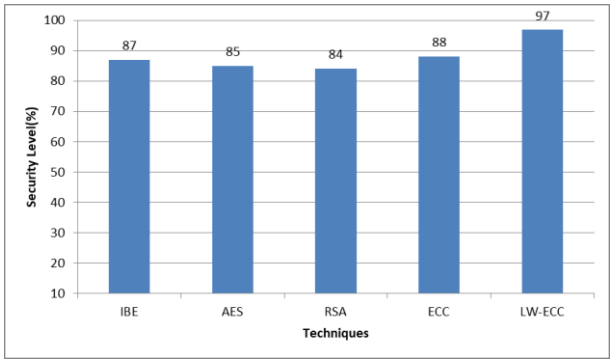
Fig. 5. Evaluation of the introduced classifier ASB-IB with other classifiers such as LSTM, CNN, SNN and BSNN in various stages of attack and non-attack



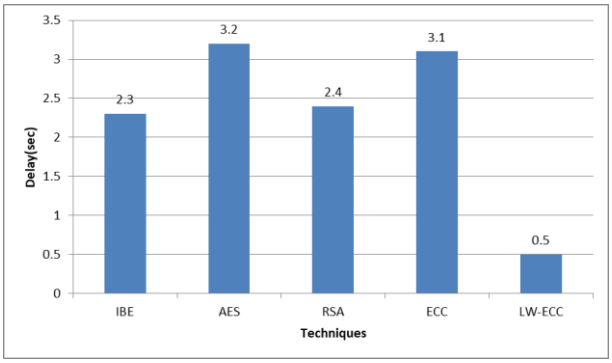
(a). Comparison of encryption time (sec)



(b). Comparison of decryption time (sec)



(c). Comparison of Security level



(d). Comparison of delay (sec)

Fig. 6. 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 Fig. 6(c) and Fig. 6(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 Fig. 6(a) and Fig. 6(b) and proven that LW-PWECC achieved a lower period of time for the process than the traditional approaches.

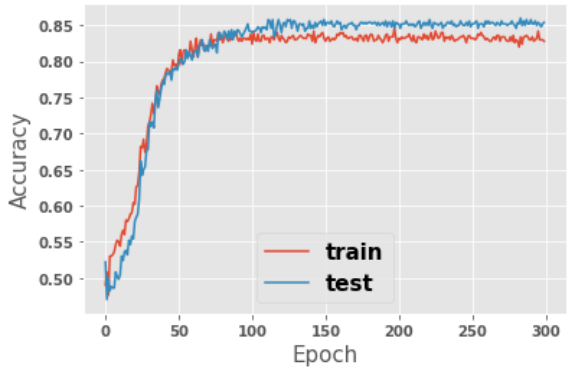
The accuracy and loss curve with the number of iterations is depicted in Fig. 7(a) and Fig. 7(b). The accuracy curve in Fig. 7(a) is depicted for about 300 iterations shows that the accuracy of training and testing is more identical and increases with increase in epochs and maintains a constant value 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 Fig. 7(b) decreases with increase in epochs. The testing loss is slightly higher for about 100 epochs and after that testing loss falls.

Fig. 8 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. The other traditional approaches used for comparing the overall accuracy such as DNN [47], MSCSL [49] also uses the ECU-IoHT dataset for attack detection and data security. This model achieves an accuracy of 99.93% which is comparatively higher than existing models as shown in Fig. 9, 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.

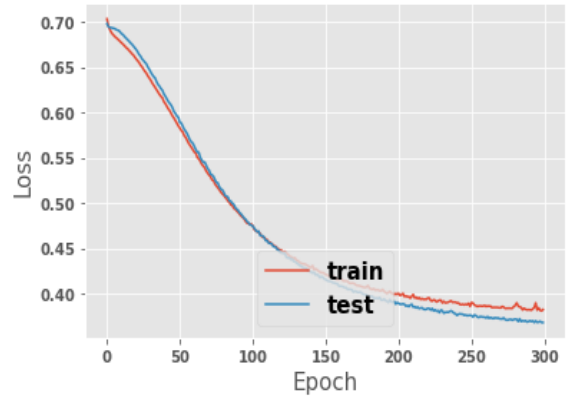
From Table III, it is verified the major problem that is motivated to do this work i.e. training instability is overcame by proposed method by solving the degradation problem. The agnostic meta learning training helps the neural network of this manuscript to improve the training stability by updating the learning rate parameter. The evaluation is done by taking the methods such as DNN, MSCSL which uses the same ECU-IoHT dataset for input data and proven that the proposed technique achieved a maximum training stability within a period of 0.028 seconds which is comparatively lower than the other techniques.

TABLE I. OVERALL COMPARISON OF MATRICES CONSIDERED WITH OTHER TECHNIQUES

Techniques	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Execution time (s)
DNN [47]	99.85	99.3	96.8	90.3	0.70
MSCSL [49]	97.90	96.78	95.90	96.54	0.65
Proposed	99.93	99.97	99	99.3	0.45



(a). Accuracy v/s Epoch



(b). Loss v/s Epoch

Fig. 7. Accuracy and loss curve with the number of iterations

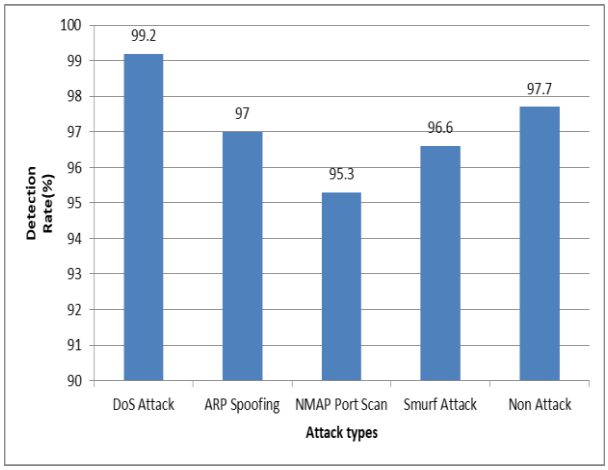


Fig. 8. Detection rate

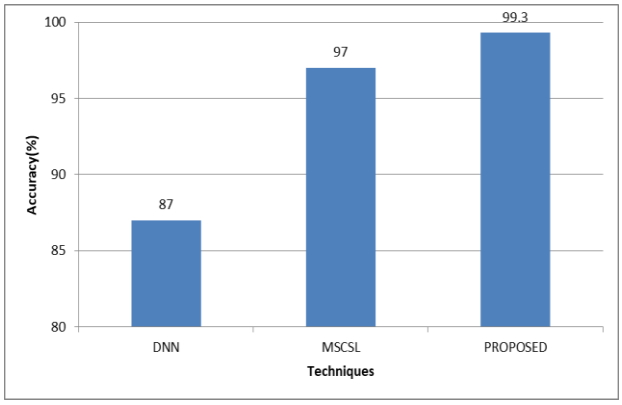


Fig. 9. Comparison of overall accuracy

IV. CONCLUSION

The ASB-IB for accurate detection of network attacks and LW-PWECC framework for secure data transmission is successfully implemented. 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 99.93%, overall lower training time of 0.028 secs with high security and minimal delay. The analyses on Mc Neymar and Wilcoxon Rank Sum tests show that the introduced model is statistically significant. However, IoHT can face a lot of challenges in near future like standard in architecture is not very well defined by policy makers, adoptability of cloud is not done adequately, various new kind of attacks can happen. The research in improvement of IoHT ecosystem has a lot of scope. The future work of the suggested approach will be done by deploying the framework in the cloud infrastructure.

ACKNOWLEDGEMENT

The authors would like to acknowledge SJB Institute of Technology and Visvesvaraya Technological University for the provision of facilities to complete this work.

REFERENCES

[1] K. Qureshi, M. Saeed, A. Ahmed, and G. Jeon, "A Novel and Secure Attacks Detection Framework for Smart Cities Industrial Internet of Things," *Sustainable Cities and Society*, vol. 61, p. 102343, 2020.

[2] F. S. de Lima Filho F. Silveira, A. Junior, G. Vargas solar, and L. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," *Security and Communication Networks*, vol. 2019, pp. 1–15, 2019.

[3] N. Velayudhan, A. Arulappan, and M. Madanan, "Sybil attack detection and secure data transmission in VANET using CMEHA-DNN and MD5-ECC," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 7, 2021.

[4] A. Chenniappan and N. Vasuki, "Trust Based DoS Attack Detection in Wireless Sensor Networks for Reliable Data Transmission," *Wireless Personal Communications*, vol. 121, no. 12 2021.

[5] J. Alzubi and Alzubi, "Bipolar fully recurrent deep structured neural learning based attack detection for securing industrial sensor networks," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, 2021.

[6] A. Tekerek, "A Novel Architecture for Web-Based Attack Detection Using Convolutional Neural Network," *Comput. Secur.*, vol. 100, p. 102096, 2021.

[7] A. Diro and N. Chilamkurti, "Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications," *IEEE Communications Magazine*, vol. 56, pp. 124–130, 2018.

[8] J. Alsamiri and K. Alsubhi, "Internet of Things Cyber Attacks Detection using Machine Learning", *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 12, 2019.

[9] A. I. Naeem Firdous Syed Zubair Baig and C. Valli, "Denial of service attack detection through machine learning for the IoT," *Journal of Information and Telecommunication*, vol. 4, no. 4, pp. 482–503, 2020.

[10] T. Gu, A. Abhishek, H. Fu, H. Zhang, D. Basu and P. Mohapatra,

"Towards Learning-automation IoT Attack Detection through Reinforcement Learning," *2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pp. 88-97, 2020.

[11] F. Alsubaei, A. Abuhussein and S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 112-120, 2017.

[12] S. M. Nagarajan, G. G. Deverajan, U. Kumaran, M. Thirunavukkarasan, M. D. Alshehri, and S. Alkhalaf, "Secure Data Transmission in Internet of Medical Things Using RES-256 Algorithm," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8876-8884, Dec. 2022, doi: 10.1109/TII.2021.3126119.

[13] R. Bosri, A. Uzzal, A. Omar, M. Bhuiyan, and S. Rahman, "HIDEchain: A User-Centric Secure Edge Computing Architecture for Healthcare IoT Devices," *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 376–381, 2020.

[14] M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, and P. Haskell-Dowland, "ECU-IoHT: A dataset for analyzing cyberattacks in Internet of Health Things," *Ad Hoc Networks*, vol. 122, p. 102621, 2021.

[15] M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, and P. Haskell-Dowland, "ECU-IoHT," *Ad Hoc Networks*, 2020.

[16] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods," in *IEEE Access*, vol. 8, pp. 152316-152332, 2020.

[17] J. Chen, Y. Zhao, J. Lin, Y. Dai, B. Hu, and S. Gao, "A Flexible Insole Gait Monitoring Technique for the Internet of Health Things," in *IEEE Sensors Journal*, vol. 21, no. 23, pp. 26397-26405, 2021.

[18] J. J. Kang, M. Dibaei, G. Luo, W. Yang, and X. Zheng, "A Privacy-Preserving Data Inference Framework for Internet of Health Things Networks," *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1209-1214, 2020.

[19] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Personal and ubiquitous computing*, pp. 1-14, 2021.

[20] C. Huang, G. Xu, S. Chen, W. Zhou, E. Y. Ng, and V. H. C. de Albuquerque, "An improved federated learning approach enhanced internet of health things framework for private decentralized distributed data," *Information Sciences*, vol. 614, pp. 138-152, 2022.

[21] A. O. Almagrabi, R. Ali, D. Alghazzawi, A. AlBarakati, and T. Khurshaid, "A Reinforcement Learning-Based Framework for Crowdsourcing in Massive Health Care Internet of Things," *Big Data*, vol. 10, no. 2, pp. 161–170, 2022.

[22] A. Rana, C. Chakraborty, S. Sharma, S. Dhawan, S. K. Pani, and I. Ashraf, "Internet of Medical Things-Based Secure and Energy-Efficient Framework for Health Care," *Big Data*, vol. 10, no. 1, pp. 18–33, 2022.

[23] Y. Qu, X. Ming, S. Qiu, M. Zheng, and Z. Hou, "An integrative framework for online prognostic and health management using internet of things and convolutional neural network," *Sensors*, vol. 19, no. 10, p. 2338, 2019.

[24] M. Kaur, D. Singh, V. Kumar, B. B. Gupta, and A. A. Abd El-Latif, "Secure and Energy Efficient-Based E-Health Care Framework for Green Internet of Things," in *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 3, pp. 1223-1231, Sept. 2021.

[25] S. Ariyanti and Kautsarina, "A Proposed The Internet of Things (IoT) Framework for Health Sector in Indonesia," *2018 IEEE Region Ten Symposium (Tensymp)*, pp. 282-286, 2018.

[26] M. A. Rahman, M. S. Hossain, A. J. Showail, N. A. Alrajeh, and M. F. Alhamid, "A secure, private, and explainable IoHT framework to support sustainable health monitoring in a smart city," *Sustainable Cities and Society*, vol. 72, p. 103083, 2021.

[27] A. Mukherjee, S. Ghosh, A. Behere, S. K. Ghosh, and R. Buyya, "Internet of Health Things (IoHT) for personalized health care using integrated edge-fog-cloud network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 943-959, 2021.

[28] M. Bansal and Priya, "Application Layer Protocols for Internet of Healthcare Things (IoHT)," *2020 Fourth International Conference on Inventive Systems and Control (ICISC)*, pp. 369-376, 2020.

[29] Q. Vu Khanh, N. Vi Hoai, A. Dang Van, and Q. Nguyen Minh, "An integrating computing framework based on edge-fog-cloud for internet of healthcare things applications," *Internet of Things*, vol. 23, p. 100907, 2023.

[30] E. C. Junior, R. M. de Castro Andrade, and L. S. Rocha, "KREATION: Kotlin Framework for Self-Adaptive IoHT Applications," *2023 IEEE 11th International Conference on Serious Games and Applications for Health (SeGAH)*, pp. 1-8, 2023.

[31] F. Farhin, M. S. Kaiser, and M. Mahmud, "Towards Secured Service Provisioning for the Internet of Healthcare Things," *2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT)*, pp. 1-6, 2020.

[32] M. I. Alam, M. O. Ahmad, S. T. Siddiqui, M. R. Khan, H. Khan, and K. A. Qidwai, "Blockchain for 5G-Enabled IoHT---A Framework for Secure Healthcare Automation," In *Proceedings of Data Analytics and Management*, pp. 793–801, 2023.

[33] B. Bai, S. Nazir, Y. Bai, and A. Anees, "Security and provenance for Internet of Health Things: A systematic literature review," *Journal of Software: Evolution and Process*, vol. 33, no. 5, p. e2335, 2021.

[34] P. Sarosh, S. A. Parah, and G. Mohiuddin Bhat, "Fast Image Encryption Framework for Medical Images," *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 149-154, 2021.

[35] A. Dutta, C. Misra, R. K. Barik, and S. Mishra, "Enhancing Mist Assisted Cloud Computing Toward Secure and Scalable Architecture for Smart Healthcare," In *Advances in Communication and Computational Technology*, pp. 1515–1526, 2021.

[36] F. Mosaiyebzadeh, S. Pouriyeh, R. M. Parizi, M. Han, and D. M. Batista, "Intrusion Detection System for IoHT Devices using Federated Learning," *IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1-6, 2023.

[37] A. K M, A. Joshy, A. T. George, and G. Gopika, "Internet of Healthcare Things (IoHT) Enabled Incessant Real Time Patient Monitoring System Using Non-Invasive Sensors," *2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 01-06, 2022.

[38] C. C. Prajapati, H. Kaur, and J. Singla, "A Comprehensive Review on Smart Fog-Based Healthcare Framework," *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 622-627, 2020.

[39] M. T. Khan, L. Barik, A. Adholiya, S. S. Patra, A. N. Brahma, and R. K. Barik, "Task Offloading Scheme for Latency Sensitive Tasks In 5G IOHT on Fog Assisted Cloud Computing Environment," *2022 3rd International Conference for Emerging Technology (INCET)*, pp. 1-5, 2022.

[40] Y. Justindhas and P. Jeyanthi, "Attack Detection and Prevention in IoT-SCADA Networks Using NK-Classifier," *Soft Comput.*, vol. 26, no. 14, pp. 6811–6823, 2022.

[41] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Federated Semi-Supervised Learning for Attack Detection in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 19, 2022.

[42] S. P. K. Gudla, S. K. Bhoi, S. R. Nayak, K. K. Singh, A. Verma, and I. Izonin, "A Deep Intelligent Attack Detection Framework for Fog-Based IoT Systems," *Computational Intelligence and Neuroscience*, vol. 2022, p. 6967938, 2022.

[43] A. Duraisamy and M. Subramaniam, "Attack Detection on IoT Based Smart Cities Using IDS Based MANFIS Classifier and Secure Data Transmission Using IRSA Encryption," *Wirel. Pers. Commun.*, vol. 119, no. 2, pp. 1913–1934, 2021.

[44] B. A. Alabsi, M. Anbar, and S. D. A. Rihan, "CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks," *Sensors*, vol. 23, no. 14, 2023.

[45] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. K. M. Najmul Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare

system," *Journal of Parallel and Distributed Computing*, vol. 172, pp. 69–83, 2023.

[46] I. Priyadarshini, P. Mohanty, A. Alkhayyat, R. Sharma, and S. Kumar, "SDN and application layer DDoS attacks detection in IoT devices by attention-based Bi-LSTM-CNN," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 11, p. e4758, 2023.

[47] K. P. Vijayakumar, K. Pradeep, A. Balasundaram, and M. R. Prusty, "Enhanced Cyber Attack Detection Process for Internet of Health Things (IoHT) Devices Using Deep Neural Network," *Processes*, vol. 11, no. 4, 2023.

[48] M. Ezhilarasi, L. Gnanaprasanambikai, A. Kousalya, and M. Shanmugapriya, "A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks," *Soft Computing*, vol. 27, 2022.

[49] T. Thulasi and K. Sivamohan, "LSO-CSL: Light Spectrum Optimizer-Based Convolutional Stacked Long Short Term Memory for Attack Detection in IoT-Based Healthcare Applications," *Expert Syst. Appl.*, vol. 232, 2023.

[50] K. S. Sankaran and B.-H. Kim, "Deep learning based energy efficient optimal RMC-CNN model for secured data transmission and anomaly detection in industrial IOT," *Sustainable Energy Technologies and Assessments*, vol. 56, p. 102983. 2023.

[51] A. Duraisamy, M. Subramaniam, and C. R. R. 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*, vol. 30, no. 2, pp. 121-131, 2021.

[52] E. Hosseini, A. Al-Shakarchi, K. Z. Ghafoor, D. B. Rawat, M. Saif, and X. Yang, "Volcano eruption algorithm for solving optimization problems," *Neural Computing and Applications*, vol. 33, pp. 2321-2337, 2020.

[53] V. -T. Nguyen, Q. -K. Trinh, R. Zhang, and Y. Nakashima, "STT-BSNN: An In-Memory Deep Binary Spiking Neural Network Based on STT-MRAM," in *IEEE Access*, vol. 9, pp. 151373-151385, 2021.

[54] X. Yao, J. Zhu, G. Huo, N. Xu, X. Liu, and C. Zhang, "Model-agnostic multi-stage loss optimization meta learning," *International Journal of Machine Learning and Cybernetics*, vol. 12, no. 8, pp. 2349–2363, 2021.

[55] A. Kaveh, M. Khanzadi, and M. Rastegar Moghaddam, "Billiards-inspired optimization algorithm; a new meta-heuristic method," *Structures*, vol. 27, pp. 1722–1739, 2020

[56] Y. Justindhas and P. Jeyanthi, "Attack Detection and Prevention in IoT-SCADA Networks Using NK-Classifier," *Soft Comput.*, vol. 26, no. 14, pp. 6811–6823, 2022.

[57] T. S. L. V. Ayyarao *et al*., "War Strategy Optimization Algorithm: A New Effective Metaheuristic Algorithm for Global Optimization," in *IEEE Access*, vol. 10, pp. 25073-25105, 2022.

[58] F. A. Zeidabadi and M. Dehghani, "POA: Puzzle Optimization Algorithm," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 1, 2022.

[59] L. Liang *et al*., "Exploring Adversarial Attack in Spiking Neural Networks with Spike-Compatible Gradient," In *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 5, pp. 2569-2583, 2023.

[60] R. Bhandari and V. B. Kirubanand, "Enhanced encryption technique for secure iot data transmission," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, p. 3732, 10 2019.

[61] M. A. Ahmed and S. Alnatheer, "Deep Q-Learning with Bit-Swapping-Based Linear Feedback Shift Register fostered Built-In Self-Test and Built-In Self-Repair for SRAM," *Micromachines*, vol. 13, no. 6, p. 971, 2022.

[62] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Applied Soft Computing*, vol. 72, pp. 79–89, 2018.

[63] S. Majumder, S. Ray, D. Sadhukhan, M. Khurram, and M. Dasgupta, "ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things," *Wireless Personal Communications*, vol. 116, pp. 1867-1896, 2021.