FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

A Deep Fusion Model For Automated Industrial Iot Cyber Attack Detection And Mitigation

Bibhuti Bhusana Behera[1], Rajani Kanta Mohanty[2], Binod Kumar Pattanayak[3]

[1]Department of Computer Science and Engineering. Institute of Technical Education and Research, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, India, bibhuti.1973@gmail.com
[2]Department of Computer Science and Engineering-SP, Jain University, Bengaluru, India, rkm.bbs@gmail.com
[3]Department of Computer Science and Engineering. Institute of Technical Education and Research, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, India, binodpattanayak@soa.ac.in

***Correspondence**: Binod Kumar Pattanayak; Email: binodpattanayak@soa.ac.in

ABSTRACT- The Industrial Internet of Things (IIoT) is a new field of study that connects digital devices and services to physical systems. The IIoT has been utilized to create massive amounts of data from various sensors, and it has run into several problems. The IIoT has been subjected to a variety of hacks, putting its ability to provide enterprises with flawless operations in jeopardy. Businesses suffer financial and reputational losses as a result of such threats, as well as the theft of critical data. As a result, numerous Network Intrusion Detection Systems (NIDSs) have been created to combat and safeguard IIoT systems, but gathering data that can be utilized in the construction of an intelligent NIDS is a tough operation; consequently, identifying current and new assaults poses major issues. In this research work, a novel IIOT attack detection framework and mitigation model is designed by following four major phases "(a) pre-processing, (b) feature extraction, (c) feature selection and (d) attack detection". Initially, the collected raw data (input) is subjected to pre-processing phase, wherein the data cleaning and data standardization operations take place. Subsequently, the features like "higher-order statistical features (Skewness, Kurtosis, Variance and Moments), technical indicator based features, mutual information, Improved Principal Component Analysis (IPCA)" based features are extracted from the pre-processed data. Further, from the extracted features, the most optimal features are selected using a new hybrid optimization model referred as Hunger Customized Individual Activity Model (HCIA) that hybrids the concepts of standard (Teamwork Optimization Algorithm (TOA) and Hunger Games Search (HGS)). The attack detection is carried out using the projected deep fusion model framework that encapsulates the Bi-GRU and Quantum Deep Neural Network (QDNN), respectively. The Bi-GRU and QDNN in the deep fusion model framework is trained with the optimal features selected using a new hybrid optimization model. The outcome acquired from Bi-GRU and QDNN is combined, and it will be the final detected outcome that portrays the presence/ absence of attacks in IIoT network. When an attack is being identified, the mitigation of such attack takes place via the Improved BIAT Framework. Further, the projected model is evaluated over the existing models to show its supremacy in the attack detection and mitigation process.

General Terms: Industrial Internet of Things (IIoT), Teamwork Optimization Algorithm (TOA)

Keywords: IIoT; Attack Detection; Deep Learning Model; Improved BAIT; HCIA

ARTICLE INFORMATION

Author(s): Bibhuti Bhusana Behera, Rajani Kanta Mohanty, Binod Kumar Pattanayak;
Received: 11/05/2022; **Accepted**: 25/07/2022; **Published**: 15/09/2022;
E- ISSN: 2347-470X;
Paper Id: IJEER220511;
Citation: 10.37391/IJEER.100332
Webpage-link:
www.ijeer.forexjournal.co.in/archive/volume-10/ijeer-100332.html

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

Automation of everything has produced a profound transformation and human flourishing in the industrial revolution. The computers have been used to interconnect real-world application management, data mining as well as digital devices [1-5]. This revolution has enabled anyone to access a huge count of information (i.e. trillion of data) that opens up new possibilities in the physical and digital industries, humans may notice significant gains, resulting in a higher quality of life and a more successful society. The IIoT is known for generating large amounts of data from numerous sensors. Healthcare, retail, automotive, and transportation are all affected by these applications. The IIoT has the potential to boost efficiency, production, and operational efficiency in a variety of sectors. The existing services are initially improved by IIoT with the ultimate goal of creating entirely intelligent and enhanced services and products [6-10]. This has enabled most of the organization to grab knowledge about how and where IIoT innovations and solutions have to lead to transformations in the organization, enhanced goods, and services quality. By merging technical breakthroughs, sensors, programs, and applications on the IIoT, machine learning, and deep learning algorithms can improve dependability, production, and customer happiness [11-14].

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

In IIoTs, M2M and M2P network connections are made utilizing the TCP/IP interface and several IIoT protocols [14, 15]. As the count of IIoTs increases, the count of the number of faults and defects that are exploited with sophisticated attack methods has dramatically grown. Attackers try to exploit these processes to steal sensitive information, commit financial money, and corrupt device resources [16-17]. It is anticipated that cyber threats to the IIoT would cost up to $90 trillion by 2030 if the cyber security domain does not identify attractive mitigation solutions for halting them [18]. In every business spheres, protecting essential services and infrastructure has become a more pressing issue, as there is indeed an expanding growth in IIoT devices. Malware that takes advantage of zero-day vulnerabilities is one of the most common threats in IIoT networks.

The criminals use several approaches, including PDR, DoS, and DDoS, to infect susceptible machines to track and modify their behaviors. For example, the Stuxnet virus targeted Iran's nuclear program in 2010, Iranian hackers broke into the ICS of a dam in New York in 2013, and the black-energy passive assault in Ukraine in 2015 was expressly comparable to around 80.000 power disruptions [19, 20]. The NIDS is critical in identifying and responding to all Internet intrusions as a network security measure. The IIoT has evolved into a critical component of today's data and information transmission machinery, prompting the necessity for global network security [21]. NIDS are frequently used to detect system traffic to protect workstation schemes against numerous grid invasions. In [22-24], the incursion is a framework for attempting to compromise the security services of an information system. In response to the challenges posed by these intrusive frameworks, researchers have been encouraged to develop novel IDSs. Several IDS have been created and enhanced in the past, but they remain vulnerable to a variety of attacks. The potential of IDS to track and foresee hostile conduct and unknown attacks has sparked a surge of interest in anomaly detection research. Current machine learning-based irregularity detection algorithms, on the other hand, have a significant false alarm rate [10]. Therefore, deep learning models can be utilized for efficient attack detection.

The major contribution of this research work is:

- To extract a new Improved Principal Component Analysis (IPCA) based feature from the pre-processed data
- To select the most optimal features for training the attack detectors using the newly projected Hunger Customized Individual Activity Model (HCIA).
- To design a novel deep fusion model with QDNN and Bi-GRU for efficient attack detection in the IIoT

The rest of this paper is arranged as: *Section 2* discusses the literature works in IIoT attack detection. *Section 3* tells about an overview of the suggested industrial IoT attack detection and mitigation model. *Section 4* discusses the acquired results. Further, this paper is concluded in *Section 5*.

2. LITERATURE REVIEW

2.1. Related works

In 2021, Nayaka *et al.* [1] have developed a reliable DL-based IIoT routing attack detection model. In RPL, the intended attacks were identified using considering the model's adversarial training. The attack detection events have been identified with the GAN-C method that has been developed by blending the GAN and SVM models, respectively. The projected model has exhibited better detection performance. But, still, the detection rate is lower. This detection rate can be enhanced by using deep learning models.

In 2022, Ikram *et al.* [2] have introduced a "two-phase IIoT traffic prediction model" for detecting the behavior of IIoT (either normal or anomalous). Initially, the features from the input data were extracted using the MNSWOA and IPM. The behavior of the network was detected with the RF. The projected model has exhibited higher detection accuracy and ROC. However, this approach is suitable for the lower volume of data alone.

In 2022, Zhang *et al.* [4] have introduced a new ARSKE in 6G-enabled IIoT for detecting the attacks in the network. The collected data were pre-processed via the smoothing method. The active attacks have been resisted effectively with Robust Secure Reconciliation technique. The projected model has exhibited higher robustness, while tested with a real-world database. But, the energy consumed for attack detection was higher.

In 2021, Sun *et al.* [6] have detected the malware attacks in IIoT with a "classified behavior graph-based intelligent detection model". The projected model has exhibited higher detection accuracy as 99.9%. On the other hand, the projected model has exhibited has been tested with a smaller sized database, and it too required a huge count of data for training purposes. Moreover, the error rate is found to be higher.

3. AN OVERVIEW OF THE SUGGESTED INDUSTRIAL IOT ATTACK DETECTION AND MITIGATION MODEL

3.1 Architectural Description

In this research work, a novel IIOT attack detection framework and mitigation model is designed by following four major phases: "(a) pre-processing, (b) feature extraction, (c) feature selection and (d) attack detection". The architecture of the projected IIoT attack detection and mitigation process is given in *Fig.1*.

Let the collected raw data from the Industrial IoT regarding the information flow (i.e. data from the considered database) be denoted as Q^{Iflow}. This Q^{Iflow} undergoes through the following stages to explore the presence/ absence of attack within it.

The collected raw data Q^{Iflow} is initially pre-processed via a data cleaning and data standardization approach. The data cleaning is undergone first and following that the standardization process is done. At the end of the data standardization, effective and meaningful data is acquired. This data is known as the pre-processed data, and it is pointed as Q^{pre}. This Q^{pre} is utilized for further processing. To

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

determine the presence/absence of attacks within the network, the features of the pre-processed data are being utilized. In this research work, the features like higher-order statistical features g^{hstat} (Skewness, Kurtosis, Variance and Moments), technical indicator g^{TI} (ATR, CMF, and CCI) based features, mutual information g^{MI}, IPCA g^{IPCA} based features are extracted from the pre-processed data. These extracted features are integrated (G), and they are utilized to train the classifiers that make the ultimate decisions regarding the presence/absence of attacks in the network. Since the computational complexity is being a major challenge; it has been overcome in this research work using selecting the optimal features (G^{opt}) from the extracted features (G). This optimal feature selection is accomplished using the newly projected hybrid optimization model that is formulated by blending the standard TOA and HGS, respectively. The detection of the attacks in the network is the key phase of this research work. The attack detection is undergone by constructing a new Deep Fusion Model. This Deep Fusion Model encloses the Bi-GRU and Quantum Deep Neural Network (QDNN), respectively. These deep learning classifiers QDNN and Bi-GRU are trained with optimal features (G^{opt}). The outcome acquired from Bi-GRU (H^{Bi-GRU}) and QDNN (H^{QDNN}) is combined (H), and it is the final detected outcome that portrays about the presence/ absence of attacks in IIoT network. When an attack is being identified in H, the mitigation of such attack takes places via the Improved BIAT Framework.

3.2. Pre-Processing: Data Cleaning and Data Standardization

The collected data Q^{Iflow} is pre-processed to transform the raw data into an effective format that could enhance the detection accuracy of the model. In this research work, Q^{Iflow} is pre-processed via data cleaning and data standardization.

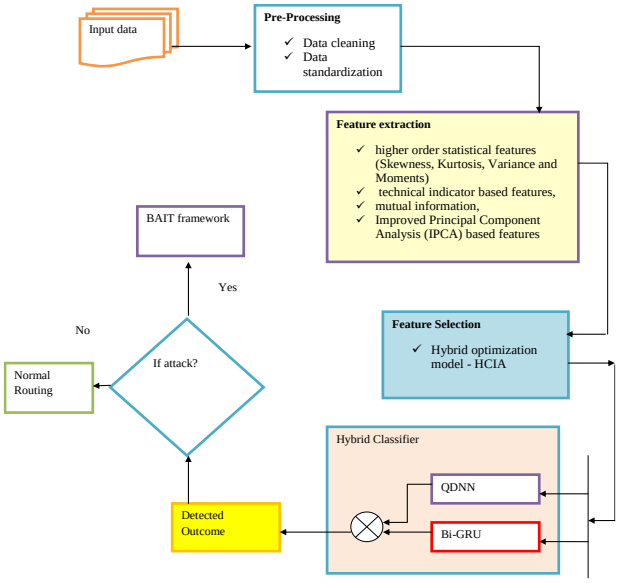

Fig. 1. The architecture of the proposed IIoT attack detection and mitigation model

Data Cleaning: the data cleaning is undergone to enhance the quality of the input data Q^{Iflow} by removing the irrelevant data within it. Moreover, the Not Available or N/A values are removed, and the missing values are filled. The data acquired after the data cleaning process is denoted as Q^{Iclean}. This Q^{Iclean} is standardized.

Data Standardization: By data standardization, Q^{Iclean} (i.e. data in diverse structures) is converted into one common format. The data standardization is undergone by mean taking the mean and standard deviation of Q^{Iclean}. The data standardization process is mathematically given in *Eq. (1).*

$$Q^{pre} = \frac{Q^{Iclean} - \mu}{\sigma} \tag{1}$$

Here, μ and σ points to the mean and standard deviation, respectively. The notation Q^{pre} denotes the pre-processed data.

3.3. Feature Extraction

The features extraction is the approach of denoting the input data into a reduced form, for making intelligent decision making. Moreover, the identification, as well as extraction of the reliable features, is indeed a crucial step. This ultimately enhances the detection accuracy. In this research work, the features like higher-order statistical features, technical indicator (ATR, CMF, and CCI) based features, mutual information, Improved Principal Component Analysis (IPCA) based features are extracted from Q_i^{pre}.

Higher-order statistical features: the higher order statistical features like Skewness, Variance, Moments, and Kurtosis, are extracted from Q^{pre}.

Skewness: the skewness provides information regarding the asymmetry of a distribution of data in $Q_i^{pre}(i=1,2,...N)$ around its mean. Mathematically, the skewness g^{skew} can be given as per *Eq. (2).*

$$g^{skew} = \frac{1}{N}\sum_{i=1}^{N}\left[\frac{Q_i^{pre} - \mu}{\sigma}\right]^3 \tag{2}$$

Kurtosis: It's a non-dimensional quantity that provides information regarding the distribution's flatness. Mathematically, the Kurtosis g^{kurt} can be given as per *Eq. (3).*

$$g^{kurt} = \left\{\frac{1}{N}\sum_{i=1}^{N}\left[\frac{Q_i^{pre} - \mu}{\sigma}\right]^4\right\} - 3 \tag{3}$$

Variance: It is the measure of the data around the central axis. Mathematically, the variance can be given as per *Eq. (4)*

$$g^{var} = \frac{1}{N-1}\left[\sum_{i=1}^{N}\left(Q_i^{pre}\right)^2 - N\mu^2\right] \tag{4}$$

Moment: It is mathematically extracted as per *Eq. (5).*

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

$$g^{mom} = \frac{\mu_k}{\sigma_k} \quad (5)$$

Here, μ_k and σ_k denotes the k^{th} moment of mean and standard deviation, respectively.

The extracted higher-order statistical features are denoted as g^{hstat}.

Technical indicator: The technical indicators like ATR, CMF, and CCI are extracted from Q^{pre}. The ATR provides information regarding the average flow of the data Q^{pre} at a particular timestamp t. The CMF provides information regarding the volume of data flow at the time stamp t, and also the high-low range of information flows of Q^{pre}. The CCI tells about the current mean flow of information. The extracted technical indicator based features is pointed as g^{TI}.

Mutual information: the mutual information tells about the statistical information between two variables (say A, B) of Q^{pre}. Mathematically, the Mutual Information based features is computed as per *Eq. (6).*

$$g^{MI}(A,B) = \sum_{A,B} p(A,B).\log\frac{p(A,B)}{p(A).p(B)} \quad (6)$$

Here, $p(A,B)$, $p(A)$ and $p(B)$ denotes their probability distribution, respectively. The extracted mutual information-based feature is pointed as g^{MI}.

Improved Principal Component Analysis (IPCA): The steps followed in IPCA based feature extraction mechanism is manifested below:

The pre-processed data Q^{pre} has m samples with n attributes.

Step 1- Initially Q^{pre} is standardized based on the harmonic mean.

$$Z_{ij} = \left(Q_{ij}^{pre} - \overline{Q_{ij}^{pre}}\right)\gamma_{ij} \;//\; i = 1,2,...N;\; j = 1,2,...M \quad (7)$$

Here, $\overline{Q_{ij}^{pre}}$ denotes the weighted harmonic mean of Q_{ij}^{pre}. Z_{ij} is the improved data standardization. This is shown in *Eq. (8)*

$$\gamma_{ij} = \max[Q_{ij}^{pre}] - \min[Q_{ij}^{pre}];\; \gamma_{ij} > 0 \quad (8)$$

Step 2- Compute the correlation coefficient matrix ϕ as per *Eq. (9)*

$$\phi = \left[\rho_{Q_i^{pre},Q_j^{pre}}\right]_{n*n} = \frac{1}{m}\varsigma^T.Q_{ij}^{pre} \quad (9)$$

Here, $\left[\rho_{Q_i^{pre},Q_j^{pre}}\right]$ denotes the correlation coefficient between Q_i^{pre} and Q_j^{pre}

Step 3- Compute the eigenvectors and Eigen values. This is done by computing $|\phi - \lambda E| = 0$

Step 4- Determine the principal components

Step 5- Identify the indicators belonging to the determined principal components compute the component score as per *Eq. (10)*

$$CF = \omega_k.f_k \quad (10)$$

In which,

$$\omega_k = \frac{\lambda_k}{\sum_{k=1}^{P}\lambda_k} * r \quad (11)$$

Here, r is a random variable that is computed using the logistic map. The extracted IPCA based features is pointed as g^{IPCA}.

All the extracted features are integrated as $G = g^{IPCA} + g^{MI} + g^{TI} + g^{hstat}$

3.4. Optimal Feature Selection

The optimal features are selected from the extracted features to reduce the computational complexity of the model. In this research work, a hybrid optimization model is introduced to for selecting the optimal features from G. The projected hybrid optimization model is the conceptual amalgamation of the standard HGS [20] and TOA [21], respectively. The HGS is based on the "hunger-driven activities and behavioral choice of animals". The TOA model has been developed with the inspiration acquired from the behavior of the members of a team, who work together in achieving the desired goal. The HGS and TOA are said to be efficient in solving complex optimization problems, and so they have been selected for conceptual leveraging. In literature, it has been suggested that the hybrid optimization model are aid in enhancing the convergence speed of the solutions [21-23]. The steps followed in the projected hybrid optimization model are manifested below:

Step 1- Initialize the position of the search agent $X_o; o = 1,2,...O$. The current iteration is denoted as itr and the maximal iteration is pointed as $\max^{itr}$.

Step 2- The algorithmic parameters $N, itr, shungry$ // N – count of individuals; $shungry$ – the sum of the hungry feeling of all the search agents.

Step 3- While $itr \le \max^{itr}$

Step 4- Compute the fitness of all the search agents using *Eq. (12).*

$$fit = \min\left(\frac{1}{Accuracy}\right) \quad (12)$$

Step 5- Update BF, WF, X_{best} // BF -so far acquired best fitness of the search agent, WF – so far acquired worst fitness of the search agent, X_{best} – location of the best individual in the iteration.

Step 6- Compute the hungry phase $hungry(i)$ as per *Eq. (13).* In this process, the individual's starvation characteristics are

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

simulated.

$$hungry(i)=\begin{cases}0 & A_{fit}(i)==BF\\ hungry(i)+H & A_{fit}(i)!=BF\end{cases} \quad (13)$$

Here, $A_{fit}(i)$ denotes the fitness of all search agents in the current iteration and H denotes the hunger.

Step 7- Compute the value of $W1$ in hunger role using *Eq. (14)*.

$$W1(i)=\begin{cases}1 & if\ rand4>1\\ hungry(i).\dfrac{N}{shungry}(rand4) & if\ rand4<l\end{cases} \quad (14)$$

Here, $rand4$ is a random number generated between [0,1].

Step 8- Compute the value of $W2$ in hunger role using *Eq. (15)*.

$$W2(i)=\left[1-\exp(-\left|hungry(i)-shungry(i)\right|)\right]*rand5*2 \quad (15)$$

Here, $rand5$ is a random number generated between [0,1].

Step 9- For every search agent

Step 10- Compute the variation control for all positions E using *Eq. (16)*.

$$E=\sec h\left[\left|obj(i)-BF\right|\right] \quad (16)$$

Here, $obj(i)$ is the fitness of the search agent

Step 11- Update R by using *Eq. (17)* and *Eq. (18)*, respectively.

$$R=2*shrink*rand-shrink \quad (17)$$

$$shrink=2*\left(1-\frac{itr}{\max^{itr}}\right) \quad (18)$$

Here, $rand$ is a random number generated between [0,1].

Step 12- Update position of the search agent using the approach food phase as per *Eq. (19)*.

$$X(itr+1)=\begin{cases}X(itr).(1+randn(1)) & rand1<l\\ W1.X_{best}+R.W2.\left|X_{best}-X(itr)\right| & rand1>l;rand2>E\\ W1.X_{best}-R.W2.\left|X_{best}-X(itr)\right| & rand1>l;rand2<E\end{cases} \quad (19)$$

Here, $rand1, rand2$ is a random number generated between [0,1]. $randn(1)$ is a random number that satisfies the normal distribution.

Step 13- Return X_{best}

Step 14- Input X_{best} into the individual activity phase of TOA model. Update the values of X_{best} using *Eq. (20)* of TOA model. In TOA, each team member tries to improve her/his performance based on her/his current situation.

$$X'_{best}=X_{best}+(-0.01+r*0.02)*X'_{best} \quad (20)$$

Moreover, the value of r is generated using the cubic map (proposed), instead of generating it randomly

Step 15- Return the acquired X'_{best} from TOA

Step 16- End while

3.5. Attack Detection with Deep Fusion Model

The attack detection is carried out using the projected Deep Fusion Mode that encapsulates the Bi-GRU and QDNN, respectively. The Bi-GRU and QDNN in the Deep Fusion Model is trained with the optimal features selected using a new hybrid optimization model. The outcome acquired from Bi-GRU and QDNN is combined, and it will be the final detected outcome that portrays the presence/ absence of attacks in IIoT network.

QDNN: The QDNNis a fully interconnected and directed belief nets. The QDNN encapsulates an input layer Y, N hidden layer U , and one output layer S. The layer Y has D_0 units equal to the feature space, and the output layer has C units equal to the count of classes in the input database. The quantum neurons are available in the last layer U^N. The QDNN can be given as per *Eq. (21)*.

$$S^t(Y)=C^t_{N+1}+\sum_{s=1}^{D_N}w^{st}_{N+1}.U^s_N(Y);t=1,2,...C \quad (21)$$

The hidden layer U^N has quantum neurons. The outcome U^N is expressed as per *Eq. (22) and Eq. (23)*, respectively.

$$U^t_N(Y)=\frac{1}{n_l}\sum_{r=1}^{n_l}sigm(z^t_N-\theta^t_N) \quad (22)$$

$$z^t_N(Y)=C^t_N+\sum_{s=1}^{D_{N-1}}w^{st}_{N+1}.U^s_{N+1}(Y) \quad (23)$$

Here,

Sigmoid function $sigm(\eta)=\dfrac{1}{1+e^{-\eta}}$ θ^t_N is the jumping position in the transfer function and the count of levels in hidden units is denoted as n_l.

The output of k^{th} hidden layer U_k is acquired as per *Eq. (24)*.

$$U_k=sigm\left[C^t_N+\sum_{s=1}^{D_{N-1}}w^{st}_{N+1}.U^s_{N+1}(Y)\right] \quad (24)$$

Here, $t=1,2,...D^k; k=2,...N-1; t=1,2,....D^1$ and w^k is the synaptic weight.

Bi-GRU: the Bi-GRU is a deep learning model, which is the extension of RNN. The current hidden node's candidate value hid^t is computed as per *Eq. (25)* and *Eq. (26)*, respectively.

$$\widehat{hid}^t=\tanh\left\{D_{\widehat{hid}^t}.\left[hid^{t-1}.V^t\right]\right\} \quad (25)$$

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

$$\widehat{hid}^{t-1} = hid^{t-1}.r^t \quad (26)$$

Here, $\widehat{hid}^t$ contains the current input's data, hid^{t-1} is the last transmitted state, and D is the weight function. Moreover, r^t is the gated control of reset gate and z^t is the gated control of update, D_r is the weight of reset gate and D_z is the weight of update gate. This is shown in *Eq. (27)* and *Eq. (28)*, respectively.

$$r^t = \omega\{D_r.[hid^{t-1}, V^t]\} \quad (27)$$

$$z^t = \omega\{D_z.[hid^{t-1}, V^t]\} \quad (28)$$

The outcome acquired from Bi-GRU (H^{Bi-GRU}) and QDNN (H^{QDNN}) is combined $H = mean(H^{Bi-GRU}, H^{QDNN})$, and it is the final detected outcome that portrays the presence/ absence of attacks in IIoT network.

BIAT based Attack Mitigation

The following are the actions taken in the Improved BAIT model:

1. First, the source node constructs BAIT-RREQ and selects a one-hop neighborhood node N at random, collaborating with it and utilizing its address as the destination address in the BAIT-RREQ packet.
2. If the source node broadcasts a bogus BAIT-RREQ to the route, the network has a malicious node. Furthermore, if any node other than N transmits the BAIT-RREP for this BAIT, then there is a malicious node in the network. The black hole list then flags the nodes as malicious and prevents them from transmitting in the future. The Improved BAIT based mitigation process is manifested in *Fig.2*.

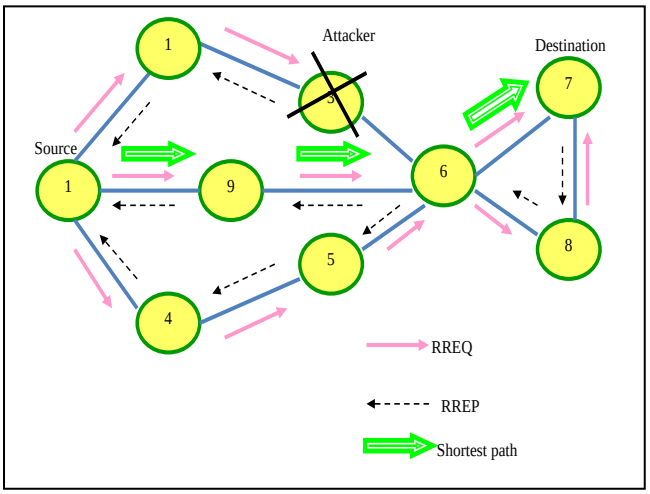

Fig. 2. Improved BAIT based attack mitigation

4. RESULTS AND DISCUSSION

4.1. Simulation procedure

PYTHON has been used as a tool to implement the proposed IIoT threat detection and mitigation methodology. Data for the evaluation was gathered from *dataset1*. The proposed model is tested against traditional models like CMBO, SMO, TOA, DHO, and HGS, respectively. The "accuracy, sensitivity, specificity, precision, NPV, F1-score and MCC, FPR, FNR, and FDR" were all included in the evaluation. The evaluation was carried out by altering the learning percentage from 40, 50, 60, 70, and 80, respectively.

4.2. Convergence Analysis

The convergence analysis is done to validate the efficiency of HCIA over the existing optimization logic in selecting the optimal features. The results acquired are revealed in *Fig.3*. On analyzing the acquired outcomes, the projected model has exhibited a lower cost function (since the fitness function for optimal feature selection is minimization function). Therefore, the projected model is said to be more applicable for selecting the optimal features.

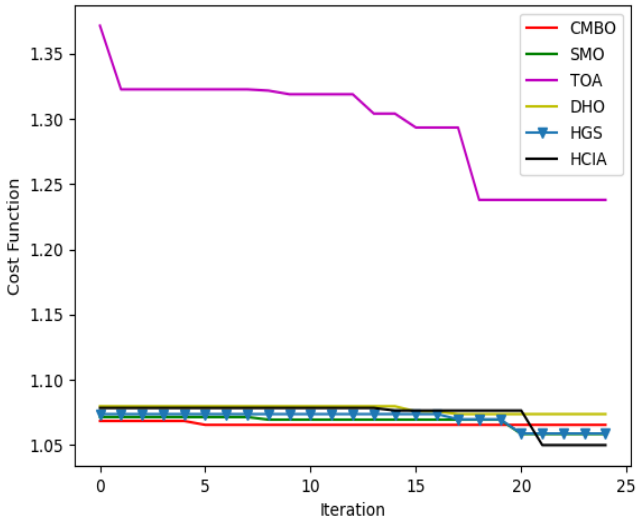

Fig. 3. Convergence Analysis

4.3. Performance Analysis

The performance analysis is undergone to validate the efficiency of the projected model. This assessment has been made in terms of "accuracy, sensitivity, specificity, precision, NPV, F1-score and MCC, FPR, FNR, and FDR", respectively. The results acquired are revealed in *Fig.4*. On analyzing the acquired outcomes, the projected model has recorded the highest accuracy as 95% at 40th learning percentage, 94.8% at 50th learning percentage, 96.2% at 60th learning percentage, and 97% at 70th learning percentage. Moreover, the projected model has rerecorded higher precision, specificity as well as sensitivity. This performance enhancement is due to the selection of the optimal features with new hybrid optimization models. Moreover, the attack detection errors are lower with the projected model, and this is due to the construction of the deep fusion model framework. Therefore, the projected model is said to be applicable for IIoT attack detection and mitigation.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

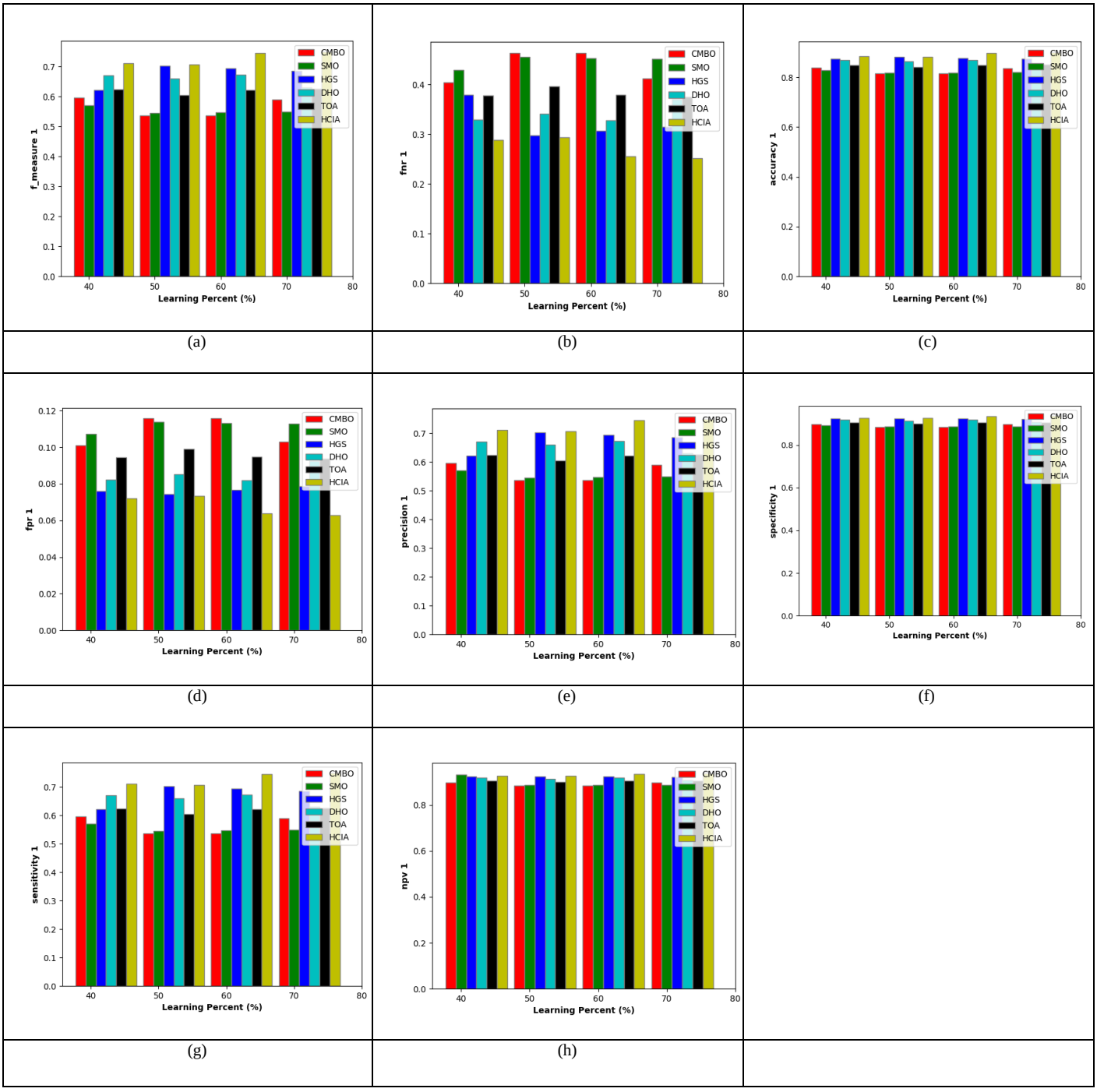

Fig. 4. Analysis on the performance of the projected model: (a) F-Measure, (b) FNR, (c) Accuracy, (d)FPR, (e) Precision, (f)Specificity, (g) Sensitivity and (h) NPV

4.4. Overall Performance Analysis

The overall performance recorded by the projected model is shown in *Table I.* here; the projected model is evaluated in terms of RNN, DBN, SVM, LSTM, CNN, proposed work without optimal feature selection, proposed work with PCA based feature extraction, and proposed work with LDA based feature extraction, respectively. on analyzing the acquired outcomes, the projected model has shown the highest accuracy as 88.2%, which is the highest value while compared to RNN=70.8%, DBN=72.3%, SVM=71.2%, LSTM=78.7%, CNN=66.1%, proposed work without optimal feature selection=81.3%, proposed work with PCA based feature extraction=67.48% and proposed work with LDA based feature extraction=78.3%. The major reason behind this improvement is due to the extraction of improved PCA-based features.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

TABLE I. OVERALL PERFORMANCE OF THE PROJECTED MODEL

Measures	RNN	DBN	SVM	LSTM	CNN	proposed work without optimal feature selection	Proposed work with PCA based feature extraction	Proposed work with LDA based feature extraction	Deep fusion model+ HCIA based feature selection and improved feature extraction
SPECIFICITY	0.818068	0.827227	0.820566	0.866986	0.788718	0.89131	0.796812	0.875034	0.92652
SENSITIVITY	0.272273	0.308909	0.282265	0.467943	0.154871	0.347861	0.187248	0.250202	0.706078
PRECISION	0.272273	0.308909	0.282265	0.467943	0.154871	0.347861	0.187248	0.250202	0.706078
NPV	0.818068	0.827227	0.820566	0.866986	0.788718	0.89131	0.796812	0.875034	0.92652
MCC	0.0903414	0.136137	0.102831	0.334929	-0.0564113	0.239171	-0.0159403	0.125235	0.632598
FPR	0.181932	0.172773	0.179434	0.133014	0.211282	0.10869	0.203188	0.124966	0.0734804
FNR	0.727727	0.691091	0.717735	0.532057	0.845129	0.652139	0.812752	0.749798	0.293922
F-MEASURE	0.272273	0.308909	0.282265	0.467943	0.154871	0.347861	0.187248	0.250202	0.706078
ACCURACY	0.708909	0.723564	0.712906	0.787177	0.661948	0.813675	0.674899	0.785772	0.882431

4.5 Statistical Performance Analysis

The statistical performance recorded by the projected model is shown in *Table II*. On analyzing the acquired outcomes, the projected model has revealed the least mean value, and this clearly shows that the projected model is less prone to detection errors.

TABLE II. STATISTICAL PERFORMANCE ANALYSIS OF THE PROJECTED MODEL

Measures	best	worst	mean	median	std
CMBO	0.171857	0.182182	0.178934	0.180849	0.00412892
SMO	0.161865	0.185179	0.174188	0.174854	0.0110311
HGS	0.149875	0.158535	0.152706	0.151207	0.00341687
DHO	0.131224	0.147877	0.136803	0.134055	0.00673306
HCIA	0.119234	0.126561	0.123564	0.12423	0.00292255

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

5.CONCLUSION

This research has introduced a unique IIOT attack detection and mitigation model. The acquired raw data (input) is first subjected to a pre-processing phase, which includes procedures such as data cleansing and standardization. The pre-processed data is then used to extract characteristics such as higher order statistical features (skewness, kurtosis, variance, and moments), technical indicator-based features, mutual information, and IPCA based features. The projected model has been evaluated over the existing models to show its supremacy in attack detection and mitigation process. On analyzing the acquired outcomes, the projected model has shown the highest accuracy as 88.2%, which is the highest value while compared to RNN=70.8%, DBN=72.3%, SVM=71.2%, LSTM=78.7%, CNN=66.1%, proposed work without optimal feature selection=81.3%, proposed work with PCA based feature extraction=67.48% and proposed work with LDA based feature extraction=78.3%. The major reason behind this improvement is due to the extraction of improved PCA based features.

APPENDIX

NOMENCLATURE

Abbreviation	Description
M2M	Machine-To-Machine
RF	Random Forest
CCI	Commodity Channel Index
IIoT	Industrial Internet Of Things
HCIA	Hunger Customized Individual Activity Model
M2P	Machine-To-Person
IDS	Intrusion Discovery Systems
NPV	Negative Predictive Value
DoS	Denial-Of-Service
CMF	Chaikin Money Flow
PDR	Progressive Determined Risk
FDR	False Discovery Rate
FPR	False Positive Rate
DDoS	Decentralized Dos
HGS	Hunger Games Search
MCC	Mathews Correlation Coefficient
IPCA	Improved Principal Component Analysis
RPL	Routing Protocol In Low-Power And Lossy Networks
ATR	Average True Range
NIDS	Network Intrusion Detection System
ARSKE	Adaptive And Robust Secret Key Extraction Scheme
FNR	False Negative Rate
TOA	Teamwork Optimization Algorithm

REFERENCES

[1] Z Sharmistha Nayaka, Nurzaman Ahmed, Sudip Misra, "Deep Learning-Based Reliable Routing Attack Detection Mechanism for Industrial Internet of Things", Ad Hoc Networks, VOl.123,2021

[2] Sumaiya Thaseen Ikram, V. Priya, B. Anbarasu, Xiaochun Cheng, Muhammad Rukunuddin Ghalib & Achyut Shankar, "Prediction of IIoT traffic using a modified whale optimization approach integrated with random forest classifier", The Journal of Supercomputing , 2022

[3] Xihua, Z. and Goyal, S.B., "Security and Privacy Challenges using IoT-Blockchain Technology in a Smart City: Critical Analysis", IJEER, Survey Report, Volume 10, Issue 2, Pages 190-195 .

[4] Lupeng Zhang,Pingchuan Wang,Fengqi Li,"An adaptive and robust secret key extraction scheme from high noise wireless channel in IIoT",Digital Communications and Networks, 2022

[5] Kumar, S., Yadav, R., Kaushik, P., Babu, S.T., Dubey, R.K. and Subramanian, M., Effective Cyber Security Using IoT to Prevent E-Threats and Hacking During Covid-19. IJEER, Research Article, Volume 10, Issue 2, Pages 111-116.

[6] Yi Sun,Ali Kashif Bashir,Fei Xiao,"Effective malware detection scheme based on classified behavior graph in IIoT", Ad Hoc Networks, 2021

[7] S. M. Kasongo, "An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms," in *IEEE Access*, vol. 9, pp. 113199-113212, 2021. doi: 10.1109/ACCESS.2021.3104113

[8] H. Cho, S. Lim, V. Belenko, M. Kalinin, D. Zegzhda and E. Nuralieva, "Application and improvement of sequence alignment algorithms for intrusion detection in the Internet of Things," *2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS)*, Tampere, Finland, 2020, pp. 93-97. doi: 10.1109/ICPS48405.2020.9274752

[9] J. Long, F. Fang and H. Luo, "A Survey of Machine Learning-based IoT Intrusion Detection Techniques," *2021 IEEE 6th International Conference on Smart Cloud (SmartCloud)*, Newark, NJ, USA, 2021, pp. 7-12. doi: 10.1109/SmartCloud52277.2021.00009

[10] Kavitha, A., Rao, B.S., Akhtar, N., Rafi, S.M., Singh, P., Das, S. and Manikandan, G., A Novel Algorithm to Secure Data in New Generation Health Care System from Cyber Attacks Using IoT. IJEER, Research Article, Volume 10, Issue 2, Pages 270-275

[11] H. Lu, T. Wang, X. Xu and T. Wang, "Cognitive Memory-Guided AutoEncoder for Effective Intrusion Detection in Internet of Things," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 3358-3366, May 2022. doi: 10.1109/TII.2021.3102637

[12] B. Naik, M. S. Obaidat, J. Nayak, D. Pelusi, P. Vijayakumar and S. H. Islam, "Intelligent Secure Ecosystem Based on Metaheuristic and Functional Link Neural Network for Edge of Things," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1947-1956, March 2020. doi: 10.1109/TII.2019.2920831

[13] F. Farivar, M. S. Haghighi, A. Jolfaei and M. Alazab, "Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2716-2725, April 2020. doi: 10.1109/TII.2019.2956474

[14] A. A. Kurniawan, H. A. Santoso, M. A. Soeleman and A. Z. Fanani, "Intrusion Detection System as Audit in IoT Infrastructure using Ensemble Learning and SMOTE Method," *2019 5th International Conference on Science in Information Technology (ICSITech)*, Yogyakarta, Indonesia, 2019, pp. 205-210. doi: 10.1109/ICSITech46713.2019.8987524

[15] P. V. Huong, L. D. Thuan, L. T. Hong Van and D. V. Hung, "Intrusion Detection in IoT Systems Based on Deep Learning Using Convolutional Neural Network," *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, Hanoi, Vietnam, 2019, pp. 448-453. doi: 10.1109/NICS48868.2019.9023871

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 604-613 | e-ISSN: 2347-470X

[16] S. H. S. Ariffin, C. J. Le and N. H. A. Wahab, "Configuring Local Rule of Intrusion Detection System in Software Defined IoT Testbed," *2021 26th IEEE Asia-Pacific Conference on Communications (APCC)*, Kuala Lumpur, Malaysia, 2021, pp. 298-303. doi: 10.1109/APCC49754.2021.9609824

[17] G. Abdelmoumin, D. B. Rawat and A. Rahman, "On the Performance of Machine Learning Models for Anomaly-Based Intelligent Intrusion Detection Systems for the Internet of Things," in *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4280-4290, 15 March15, 2022. doi: 10.1109/JIOT.2021.3103829

[18] N. Sehatbakhsh *et al*., "REMOTE: Robust External Malware Detection Framework by Using Electromagnetic Signals," in *IEEE Transactions on Computers*, vol. 69, no. 3, pp. 312-326, 1 March 2020. doi: 10.1109/TC.2019.2945767

[19] M. M. Moussa and L. Alazzawi, "Cyber Attacks Detection based on Deep Learning for Cloud-Dew Computing in Automotive IoT Applications," *2020 IEEE International Conference on Smart Cloud (SmartCloud)*, Washington, DC, USA, 2020, pp. 55-61. doi: 10.1109/SmartCloud49737.2020.00019

[20] Mohammad Dehghani and Pavel Trojovský,"Teamwork Optimization Algorithm: A New Optimization Approach for Function Minimization/Maximization", Sensors, 2021

[21] Yang, Y., Chen, H., Heidari, A. A., & Gandomi, A. H, "Hunger games search:Visions, conception, implementation, deep analysis, perspectives, and towards performance shifts", Expert Systems with Applications, Vol.155, 2021

[22] Malige Gangappa,Kiran Mai C,Sammulal P, "Enhanced Crow Search Optimization Algorithm and Hybrid NN-CNN Classifiers for Classification of Land Cover Images", Multimedia Research, Vol.2,No.3, pp.12-22,2019.

[23] kulkarni,Senthil Murugan T, "Hybrid Weed-Particle Swarm Optimization Algorithm and C- Mixture for Data Publishing", Multimedia Research, Vol.2,No.3, pp.33-42,2019."

[24] Santosh Kumar B. P,Venkata Ramanaiah K., "An Efficient Hybrid Optimization Algorithm for Image Compression", Multimedia Research, Vol.2,No.4, pp.1-11,2019.