Utilitas Mathematica
ISSN: 0315-3681 Volume 122, 2025

Bayesian Kriging Regressive Similarity Index Deep Highway Transfer Learning Network for Efficient Cyber Attack Detection in Wireless Networks

AUTHOR 1:
DHIVYA. R,
PHD PART TIME,
DEPARTMENT OF COMPUTER SCIENCE,
GOBI ARTS & SCIENCE COLLEGE ,
KARATTATIPALAYAM,
GOBICHETTIPALAYM,
ERODE(DT).

AUTHOR 2:
DR. B. SRINIVASAN,
ASSOCIATE PROFESSOR,
DEPARTMENT OF COMPUTER SCIENCE,
GOBI ARTS & SCIENCE COLLEGE ,
KARATTATIPALAYAM,
GOBICHETTIPALAYM,
ERODE(DT).

1. ABSTRACT

Wireless Network has integrated sensing technology and wireless communication for gathering the sensed data. Security attacks have major concern in wireless sensor networks (WSNs). Many researchers carried out on efficient cyber attack detection in WSN. But, the attack detection accuracy was not improved and time complexity was not minimized by existing methods. To address these issues, Bayesian Kriging Regressive Similarity Index Deep Highway Transfer Learning Network (BKRSIDHTLN) Method is introduced to perform efficient cyber attack detection with high accuracy and minimum time. Deep transfer learning involves adapting a pre-trained highway network for attack detection. Deep Highway Network collects the number of data samples and their features as input. After that, the feature selection is performed using Bayesian Kriging Regression to select the more relevant features. Then, node classification is performed for classifying the data samples for cyber attack detection. After the classification process, the fine tuning process is carried out employing artificial fish swarm optimization for enhancing the attack detection results with minimum error. After that, the Lamport Signcryption is used for securely transmitting the normal data samples. The cryptographic technique performs key generation, signcryption, and unsigncryption. During the key generation process, pair of public key and private keys is generated. Then, the signcryption is carried out using encryption and signature generation. Next, unsigncryption is performed by using signature verification and decryption to get the original data. With this, secured data transmission is achieved in wireless networks. Experimental evaluation of

BKRSIDHTLN Method is carried out on several metrics. The proposed BKRSIDHTLN Method attains better accuracy, integrity and confidentiality with lesser time.

Keywords: Wireless networks, Bayesian Kriging Regression, attack detection, confidentiality, fine tuning

2. INTRODUCTION

Wireless sensor networks (WSNs) are essential one for efficient data collection and monitoring. Every sensor node is small and simple to implement. WSN are susceptible to different security attacks and threats. A machine learning-based selective attack mitigation model was designed in [1] to identify the DoS attacks on wireless networks. However, the attack detection accuracy was not improved by designed model. Covariance Linear Learning Embedding Selection (CL2ES) methodology was introduced in [2] to extract the features for attack detection. KDBC classified the attacks depending on probability distribution value. However, the attack detection time was not reduced by CL2ES methodology. Cluster-Based Wireless Sensor Network and Variable Selection Ensemble Machine Learning Algorithms (CBWSN_VSEMLA) was designed in [3] for addressing the security threats through DoS attack detection.

A distributed framework depending on deep learning (DL) was introduced in [4] to prevent different vulnerability sources under protection system. But, the error rate was not reduced by DL method. A novel approach was introduced in [5] to identify the false data injection attack (FDIAs) through Wavelet transform and Support Vector Machines (SVMs). But, the time complexity was not reduced. Enhanced Single Valued Model based Heuristic Search on Attack Detection (ESVM-HSAD) model was introduced in [6] for Industrial applications. ESVM-HSAD method employed Grey Wolf Optimizer (GWO) to choose the optimal features. However, the data confidentiality level was not improved by ESVM-HSAD model.

An advanced Deep Learning (DL) anomaly-based technique was introduced in [7] with sensor data for identifying the network traffic statistics. But, the precision level was not improved by DL anomaly-based technique. A new real-time system was introduced in [8] for DoS/DDoS attack detection. But, the complexity level was not reduced by designed system. Multi-Stage Cyber Intelligence (MSCI) technique was introduced in [9] to find the multi-stage cyber attacks.

However, the data integrity level was not improved by MSCI technique. The safe localization and routing threat detection method was carried out in [10] for optimal distance, position and data communication. But, the attack detection accuracy was not improved by designed method.

A fuzzy model was designed in [11] with Deep Long Short-Term Memory (LSTM) algorithm for attack detection in WSNs. However, the attack detection time was not reduced by fuzzy model. An intrusion detection system was introduced in [12] with Improved deep neural network (IDNN) for improving detection performance. But, the complexity level was not reduced by designed system. A lightweight machine learning detection approach was introduced in [13] depending on decision tree with feature selection for DoS attack detection in WSNs. Soft Swish (SS)-Linear Scaling-centered Adam Convolution Neural Network (SS-LSACNN) was designed in [14] for finding the attack with compliment shift reverse operation. A general method was designed in [15] for trustworthiness computation to identify measurable Quality of Service (QoS) features. An energy-efficient ordered transmission (EEOT) scheme was introduced in [16] to identify the data falsification attacks.

The issues identified from the literature are lesser attack detection accuracy, higher attack detection time, higher computational cost, lesser data confidentiality rate, lesser data integrity rate, higher computational overhead and so on. In order to address these issues, a new method called Bayesian Kriging Regressive Similarity Index Deep Highway Transfer Learning Network (BKRSIDHTLN) Method is introduced.

The main contribution of the article is given as:

- The key aim of BKRSIDHTLN Method is to perform efficient cyber attack detection with high accuracy and minimum time consumption. Deep Highway Network architecture in BKRSIDHTLN Method collects the number of data samples and their features.
- The feature selection is carried out in BKRSIDHTLN Method using Bayesian Kriging Regression analysis to select the more relevant features for performing attack detection.
- Zijdenbos similarity index is used for analyzing the data samples of selected features with the testing data points for the cyber attack detection. Depending on the similarity value, data samples are classified into normal and attack nodes.

- The information from previously learned classification by pre-trained model is transferred into new model to significantly improve the attack detection performance. The fine tuning process is carried out in BKRSIDHTLN Method for enhancing the attack detection results with minimum error rate.
- Lamport Signcryption is used in BKRSIDHTLN Method for securely transmitting data packets with normal nodes. The cryptographic technique performs key generation, signcryption, and unsigncryption. With this, secure data transmission is performed in wireless networks.
- The result analysis is carried out on metrics like data confidentiality rate, integrity rate, attack detection accuracy and attack detection time with respect to different number of data samples.

1.1 Paper Organization:

The remaining part of this article is arranged into different sections: Section 2 reviews the related works. Section 3 outlines the proposed BKRSIDHTLN Method along with a clear architecture diagram. Section 4 elaborates the experimental settings and description of the dataset. Section 5 presents the performance assessment of the proposed BKRSIDHTLN Method in comparison with existing techniques. Lastly, Section 6 concludes the paper.

3. RELATED WORKS

DoS attack detection mechanism was introduced in [17] to guarantee the network availability and to protect the data. The designed mechanism increased DoS attack detection performance with minimum time consumption. A sophisticated Network Intrusion Detection System (NIDS) was designed in [18] to protect the cyber threats like impersonation, flooding, and injection attacks.

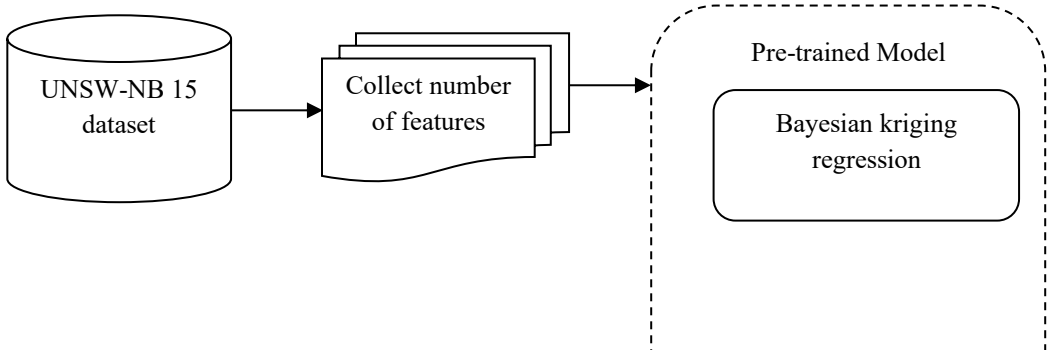
A spoofing attack detection scheme was introduced in [19] with phase difference. A graph recurrent neural network (GRNN)-based approach was introduced in [20] for identifying the eavesdropping attacks in wireless communication systems. A deep denoising autoencoder (DAE)-based framework was introduced in [21] for dimensionality reduction for high-dimensional data. Multi-Criteria Decision Making (MCDM) approach was introduced in [22] with fuzzy TOPSIS-based method for increasing the network security against DDoS attacks.

The security monitoring technology was introduced in [23] for intelligent electronic devices for security assessment. The security monitoring index system considered the running state, network traffic, and abnormal behaviors. Federated Learning approach was designed in [24] for Supervisory Control and Data Acquisition subsystems. A Lightweight, and Efficient Trust-based Mechanism (LETM-IoT) was introduced in [25] for eliminating the Sybil attacks. LETM-IoT reduced the storage and time complexity.

A cyber-attacks detection system was designed in [26] with intelligent hybrid model. The designed model increased attack detection speed. A new approach was introduced in [27] for identifying the cyber-attacks in IoT environments. The designed approach improved security level through accurately identifying the threats. Cyberattack Identification through Ensemble Deep Learning was designed in [28] for IoT environment. The network traffic data were preprocessed to eliminate irrelevant data from database. An improved security mechanism was introduced in [29] for improving the security level with minimum bit error rate for wireless sensor networks. Knowledge-Based Route Mutation (KBRM) mechanism was introduced in [30] for improving the security and adaptability in WSNs. KBRM used reinforcement learning process for attack detection.

4. METHODOLOGY

The feature selection and data classification is carried out to enhance the accuracy of cyber attack prediction. The proposed BKRSIDHTLN Method utilizes the transfer learning model for cyber attack prediction. Transfer learning is a deep learning architecture used for accurate cyber attack prediction. Transfer learning utilizes the knowledge gained from one task to enhance attack detection performance. Transfer learning enables the use of pre-trained models to adapt to new and related tasks with the minimum data. Many researchers carried out their research on cyber attack detection. But, the attack detection accuracy was not improved and detection time was not reduced. In order to address these issues, BKRSIDHTLN Method is introduced. The architecture diagram of BKRSIDHTLN Method is illustrated in figure 1.



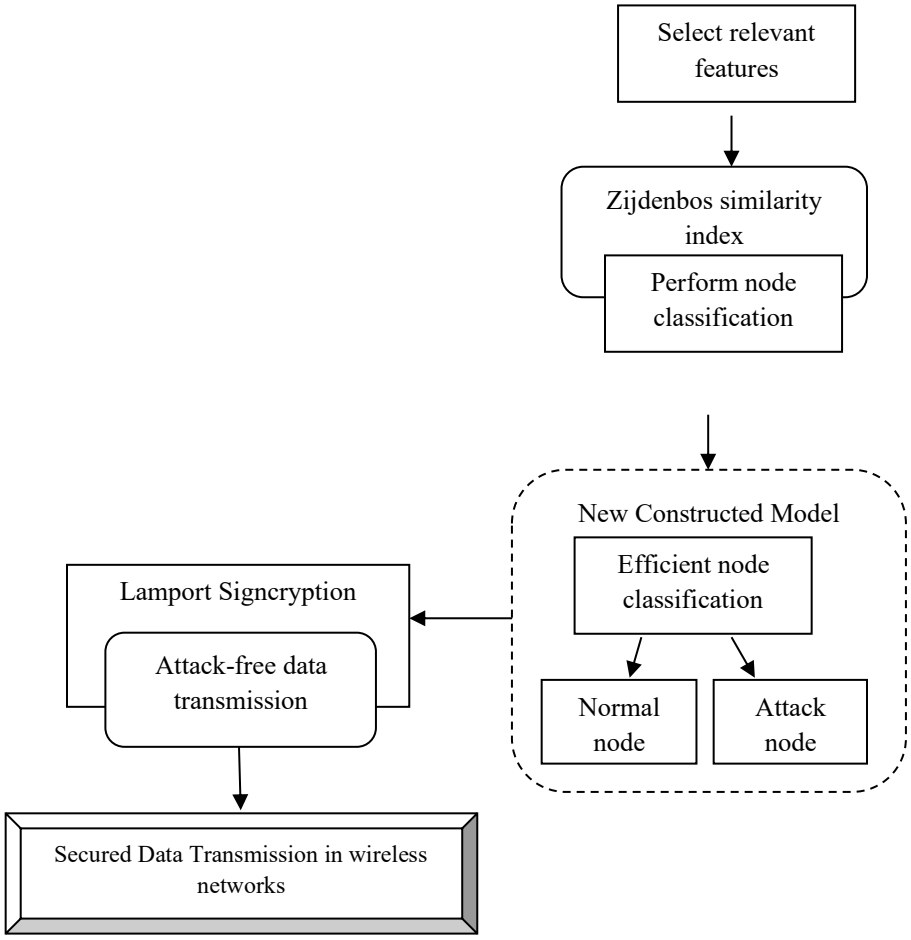


Figure 1 Architectural Diagram of BKRSIDHTLN Method

Figure 1 illustrates the architecture diagram of the proposed BKRSIDHTLN Method for accurate cyber attack prediction. BKRSIDHTLN Method is composed of two key phases namely pre-trained model construction and new model construction. In initial phase, a pre-trained model is introduced with large number of training data samples gathered from input dataset. The second phase of BKRSIDHTLN Method constructs the new model that integrates knowledge transferred from pre-trained model. These two phases are integrated into the BKRSIDHTLN Method including four fundamental processes namely data acquisition, feature selection, and classification for achieving accurate cyber attack prediction. The mixture of pre-trained and transfer learning guaranteed that BKRSIDHTLN Method is robust and adaptable for addressing the accurate cyber attack prediction.

3.1 Dataset Acquisition

The data is collected from UNSW-NB 15 dataset. The URL of the dataset is given as https://research.unsw.edu.au/projects/unsw-nb15-dataset. The network packets of UNSW-NB 15 dataset is generated by Cyber Range Lab. The dataset is used for generating the normal activities and attack behaviors. The tcpdump tool is used to collect 100 GB of raw traffic. The dataset comprised nine types of attacks, namely Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms. Argus and Bro-IDS tools are used and twelve algorithms are developed to generate 49 features with class label. The features are illustrated in UNSW-NB15_features.csv file. The number of records is two million and 540,044 are stored in four CSV files, namely UNSW-NB15_1.csv, UNSW-NB15_2.csv, UNSW-NB15_3.csv and UNSW-NB15_4.csv. The ground truth table is considered as UNSW-NB15_GT.csv and list of event file is termed as UNSW-NB15_LIST_EVENTS.csv. A partition from dataset is configured as a training set and testing set namely, UNSW_NB15_training-set.csv and UNSW_NB15_testing-set.csv respectively. The number of records is 175,341 records and testing set is 82,332 records from diverse types, namely attack and normal.

Table 1 Features of UNSW-NB15 dataset

No	Name	Type	Description
1	Srcip	nominal	Source IP address
2	Sport	Integer	Source port number
3	Dstip	nominal	Destination IP address
4	Dsport	Integer	Destination port number
5	Proto	nominal	Transaction protocol
6	State	nominal	State and its dependent protocol like ACC, CLO, CON, ECO, ECR, FIN, INT, MAS, PAR, REQ, RST, TST, TXD, URH, URN, and (-) (if not used state)
7	Dur	Float	Record total duration
8	Sbytes	Integer	Source to destination transaction bytes
9	Dbytes	Integer	Destination to source transaction bytes
10	Sttl	Integer	Source to destination time to live value

11	Dttl	Integer	Destination to source time to live value
12	Sloss	Integer	Source packets retransmitted or dropped
13	Dloss	Integer	Destination packets retransmitted or dropped
14	Service	nominal	http, ftp, smtp, ssh, dns, ftp-data ,irc and (-) if not much used service
15	Sload	Float	Source bits per second
16	Dload	Float	Destination bits per second
17	Spkts	Integer	Source to destination packet count
18	Dpkts	Integer	Destination to source packet count
19	Swin	Integer	Source TCP window advertisement value
20	Dwin	Integer	Destination TCP window advertisement value
21	Stcpb	Integer	Source TCP base sequence number
22	Dtcpb	Integer	Destination TCP base sequence number
23	Smeansz	Integer	Mean of the ?ow packet size transmitted by the src
24	Dmeansz	Integer	Mean of the ?ow packet size transmitted by the dst
25	trans_depth	Integer	Represents the pipelined depth into the connection of http request/response transaction
26	res_bdy_len	Integer	Actual uncompressed content size of the data transferred from the server's http service.
27	Sjit	Float	Source jitter (mSec)
28	Djit	Float	Destination jitter (mSec)
29	Stime	Timestamp	record start time
30	Ltime	Timestamp	record last time
31	Sintpkt	Float	Source interpacket arrival time (mSec)
32	Dintpkt	Float	Destination interpacket arrival time (mSec)
33	Tcprtt	Float	TCP connection setup round-trip time, the sum of 'synack' and 'ackdat'.
34	Synack	Float	TCP connection setup time, the time between the SYN and the SYN_ACK packets.

35	Ackdat	Float	TCP connection setup time, the time between the SYN_ACK and the ACK packets.
36	is_sm_ips_ports	Binary	If source (1) and destination (3)IP addresses equal and port numbers (2)(4) equal then, this variable takes value 1 else 0
37	ct_state_ttl	Integer	No. for each state (6) according to specific range of values for source/destination time to live (10) (11)
38	ct_flw_http_mthd	Integer	No. of flows that has methods such as Get and Post in http service
39	is_ftp_login	Binary	If the ftp session is accessed by user and password then 1 else 0
40	ct_ftp_cmd	Integer	No of flows that has a command in ftp session
41	ct_srv_src	Integer	No. of connections that contain the same service (14) and source address (1) in 100 connections according to the last time (26)
42	ct_srv_dst	Integer	No. of connections that contain the same service (14) and destination address (3) in 100 connections according to the last time (26)
43	ct_dst_ltm	Integer	No. of connections of the same destination address (3) in 100 connections according to the last time (26)
44	ct_src_ ltm	Integer	No. of connections of the same source address (1) in 100 connections according to the last time (26)
45	ct_src_dport_ltm	Integer	No of connections of same source address (1) and the destination port (4) in 100 connections based on last time (26)
46	ct_dst_sport_ltm	Integer	No of connections of similar destination address (3) and source port (2) in 100 connections based on last time (26)

47	ct_dst_src_ltm	Integer	No of connections of the same source (1) and the destination (3) address in 100 connections based on last time (26)
48	attack_cat	nominal	Attack category e.g. Fuzzers, Analysis, Backdoors, DoS Exploits, Generic, Reconnaissance, Shellcode and Worms
49	Label	Binary	0 for normal and 1 for attack records

3.2 Highway Network based Cyber Attack Detection

Highway Network is considered as the deep feedforward neural network with number of layers. The highway network employs the skip connections used through gating mechanisms to normalize the information flow. Let us consider the number of data points as $sn_i = sn_1, sn_2, sn_3, \ldots sn_n$. Highway network has the ability to avoid the gradient issues through optimization performance enhancement. Gating mechanism is used to assist the information flow across diverse layers. The highway network model has two gates with non-linear transfer functions, namely transform gate and carry gate. The carry gate is defined as,

$$C(W_c, sn) = 1 - T(W_T, sn) \qquad (1)$$

From (1), the carry gate is defined. The transform gate is a gate with the sigmoid transfer function. Initially, the number of sensor nodes is collected from the input. After that, the sensor nodes are transmitted to the hidden layer 1. In that layer, the feature selection process is carried out to bayesian kriging regression analysis. The proposed BKRSIDHTLN Method used feature selection concept for selecting the relevant features to perform efficient attack detection. The feature selection process is carried out using bayesian kriging regression function. Bayesian kriging regression analysis is a machine learning technique employed for determining the relationships between two features. Initially, number of features from input database is considered as the input. Let us consider the features as '$Ft = ft_1, ft_2, ft_3, \ldots . ft_m$.'. After that, the relationship between features is identified to eliminate the repeated features for performing efficient attack detection in wireless networks. Bayesian kriging regression is the machine learning concept used to analyze the respective feature values. It is formulated as,

$$BKR = e^{\left(\frac{Ft_i - Ft_j}{2d^2}\right)} \qquad (2)$$

From (2), 'BKR' denotes a Bayesian regression function. 'Ft_i' symbolizes the i[th] feature from input database. 'Ft_j' denotes j[th] feature from input database. 'd' symbolizes the variation. Bayesian kriging regression obtains the value varies from 0 to 1.

$$RO = \begin{cases} BKR > Th\ ; & Similar\ features \\ Otherwise; & Dissimilar\ features \end{cases} \qquad (3)$$

From (3), 'RO' represent the regression output. 'Th' symbolizes the threshold. When the regression outcome is higher than the threshold, then the feature is said to be similar feature. Otherwise, the feature is said to be dissimilar feature. After that, the selected features are carried to the hidden layer 2. In that layer, node classification is carried out using Zijdenbos similarity index. Zijdenbos similarity index is the similarity measure used to compute the relation between the selected features of the testing and training sensor nodes for efficient cyber attack detection in wireless networks. The Zijdenbos similarity index is computed as,

$$ZSI = 1 - 2 * \left[\frac{trn_f \cap tn_f}{trn_f \cup tn_f}\right] \qquad (4)$$

From (4), 'ZSI' symbolizes the cyber attack detection. 'trn_f' denotes the training node features from dataset. 'tn_f' symbolizes the testing node features. The intersection symbol '$\cap$' represents the mutual dependence between the testing and training features. The union symbol '$\cup$' represents the features in the rough set. The similarity index (SI) represents the integer value varies from '0' to '1'. Depending on the similarity value, the sensor nodes get classified into normal node and attack nodes (i.e., Fuzzers node, Analysis node, Backdoors node, DoS node, Exploits node, Generic node, Reconnaissance node, Shellcode node and Worms node). After that, the hidden layer structure in Highway Network is formulated as,

$$HO = H(W_c, sn).T(W_c, sn) + sn.(1 - T(W_T, sn)) \qquad (5)$$

From (5), 'HO' symbolizes the hidden layer output. '$H(W_c, sn)$' symbolizes the highway network output. '$T(W_c, sn)$' symbolizes the transform gate output. Then, the node classification result is carried out to the output layer for performing the attack detection in wireless networks. Finally,

the node classification output is displayed in the output layer. The algorithmic steps for highway network pre-trained model is given as,

// Algorithm 1: Highway Network Pre-trained model

Input: Dataset, number of sensor nodes '$sn_1, sn_2, sn_3, \ldots sn_n$', number of features '$ft_1, ft_2, ft_3, \ldots ft_m$'

Output: Classify the sensor nodes

Begin

1. **Collect number of sensor nodes at the input layer**
2. **For each training** samples
3. Measure bayesian kriging regression analysis between features at hidden layer 1
4. **If** ($BKR > Th$) **then**
5. Select the significant features
6. **Else**
7. Remove other features
8. **End if**
9. **For each** training and testing data samples
10. Measure the Zijdenbos similarity index at hidden layer 2
11. Classify the sensor nodes
12. Display the classification results at output layer
13. **End for**

End

Algorithm 1 explains the sensor node classification based attack detection by constructing the pre-trained classification model. A large number of sensor nodes are collected from the dataset. Then, the transfer learning model builds the pre-trained classifier for examining the input data samples. At first, the training samples are transmitted to the input layer of highway network. For every input, weights and biases are allocated to the next neuron. After that, the relevant features are chosen and irrelevant features are eliminated through regression analysis. With the selected features, node classification is carried out for performing the attack detection through examining the training and testing features of sensor nodes. Finally, classification results output is displayed at the output layer for generating multi-class classification results such as normal and attack nodes

like Fuzzers node, Analysis node, Backdoors node, DoS node, Exploits node, Generic node, Reconnaissance node, Shellcode node and Worms node)

3.3 Transfer learning model

The sensor node is taken as input to construct the new transfer learning model. In transfer learning, frozen layers represent the pre-trained model layers that remain unchanged when generating new model. Frozen layers are employed to preserve the learned features of pre-trained model. The new layers are linked for fine-tuning and output layer. The small number of sensor nodes is transmitted to the input layers and three hidden layers of pre-trained model termed frozen layers. The key objective of frozen layer enhanced the speed of training process and reduces the classification time.

In new pre-trained model, the network architecture comprised three types of layers, namely input layer, one or more hidden layers, and an output layer. The feature selection is performed in BKRSIDHTLN Method in first hidden layer using Bayesian Kriging Regression analysis to select the more relevant features. Then, Zijdenbos similarity index is used in hidden layer 2 for analyzing selected features of sensor nodes with the testing sensor node for the cyber attack detection. With the similarity value, data samples are categorized into normal and attack nodes. The input and three hidden layers are taken as the freeze layer and added one layer for performing fine tuning process to reduce the classification error. Finally result displayer in output layer.

The output of the freeze layer gets is fine tuned by applying artificial fish swarm optimization to reduce the error. For every obtained result, the error value is computed depending on the squared difference between actual outcome and prediction result. It is formulated as,

$$Error\ value = [Actual - Predicted]^2 \qquad (6)$$

From (6), '$Error\ value$' represent the error rate depending on the actual classification results. During the fine-tuning process, the hyper parameters (i.e. weight) are adjusted to improve the classification accuracy through gradient method. It is formulated as,

$$We_{t+1} = CWe_t - \eta \left[\frac{\partial error}{\partial CWe_t}\right] \qquad (7)$$

From (7), 'W_{t+1}' represent the updated weight. 'CWe_t' symbolizes the current weight. 'η' represents the learning rate, '$\frac{\partial Error}{\partial CWe_t}$' symbolizes the partial derivative of the error for

current weight. For identifying the optimal weight, artificial fish swarm algorithm is used for improving the classification performance in terms of accuracy and time. Artificial Fish Swarm Optimization is swarm intelligence algorithm based on artificial fish behavior. The behavior is based on the food search. The artificial fish swarm optimization algorithm is used to present faster convergence with higher adaptability. The artificial fish swarm optimization algorithm functioned based on the fish behavior like prey, swarm, and follow action. The artificial fish denotes the number of weights and the food source represents the classification error. Initially, number of artificial fish (i.e. weights) is initialized in the search space. It is given as,

$$We_k = We_1, We_2, We_3, \ldots . We_k \qquad (8)$$

From (8), 'We_k' represent the 'k' number of updated weighs. For every artificial fish (i.e. weight), the fitness is computed depending on the error value. The fitness function is calculated as,

$$f(We_k) = arg\ min\ Error \qquad (9)$$

From (9), '$f(We_k)$' represent the fitness of weight. '$arg\ min$' represent the argument of minimum function. '$Error$' symbolizes the error rate of classifier. Depending on the fitness estimation, the current best weight is chosen from initial population. The fitness value is determined through three behaviors, namely search, swarm, and follow for finding the global best solution.

Search Behavior of Fish

Prey is considered as an essential behavior of the artificial fish to locate the food sources. The fish identify the existence of food in water with help of vision perception. Let us consider, the current position of fish is 'F_i' and the updated position of fish is 'F_{i+1}'. When the fitness of one fish is higher than other fish (i.e., $f(F_i) < f(F_j)$), the fish performed the search or prey behavior through updating their position. It is formulated as,

$$F_{i+1} = F_i + r * s * \left(\frac{(F_j - F_i)}{\|F_j - F_i\|}\right) \qquad (10)$$

From (10), 'F_{i+1}' represent the updated position of fish. 'F_i' symbolizes the current position of fish. 'r' represents the random number ranges from zero to one. 's' symbolizes the step

of fish moving. '$\|F_j - F_i\|$' symbolizes the distance between 'j^{th} fish position and 'i^{th}' fish position.

Swarm behavior of Fish

In fish swarm behavior, fish are clustered together to reduce the risks. Let current position of fish as 'F_i' and 'F_C' denote the central position of fish. The swarm behavior of artificial fish is carried out when '$f(F_C) < f(F_i)$ && $\left(\frac{N_n}{N} < \varphi\right)$'. '$f(F_C)$' represent the fitness of artificial fish at center position. 'N_n' denotes the number of neighbors in current neighborhood. 'N' denotes the number of fishes. 'φ' symbolizes the crowd factor values varied from 0 to 1. The center of fish group has the higher food concentration with better fitness value. Consequently, the artificial fish position is updated by,

$$F_{i+1} = F_i + r * s * \left(\frac{(F_C - F_i)}{\|F_C - F_i\|}\right) \quad (11)$$

From (11), '$\|F_C - F_i\|$' represent visual distance between 'i'th position of fish and central position of fish 'F_C'

Follow Behavior of Fish

During fish swarm movement, if one or more fish identifies the food source, the fish get surrounded quickly to track and meet on food source at fast speed. Let 'F_i' denotes the current fish position and neighborhood position 'X_N'. If$(F_N) > f(F_i)$ && $\left(\frac{N_n}{N} < \varphi\right)$, follow behavior is executed. The neighboring fish 'F_N' state has higher fitness value. Depending on follow behavior, the position update is formulated as,

$$F_{i+1} = F_i + r * s * \left(\frac{(F_{max} - F_i)}{\|F_{max} - F_i\|}\right) \quad (12)$$

From (12), 'F_{i+1}' symbolizes the updated position of artificial fish. 'F_i' symbolizes the current position. 'F_{max}' denotes the position with maximum fitness function. '$\|F_{max} - F_i\|$' symbolizes the distance between position of the 'i'th fish and central position of fish with maximum fitness function 'F_{max}'. The old fish gets replaced into new optimal one depending on the fitness value. This process gets repeated until the maximum number of iterations gets reached.

Lastly, optimal weight is chosen for improving the classification accuracy with minimum time consumption. Therefore, the accurate multiple classification outcomes of the attack detection in wireless network results are obtained at the output layer. The algorithmic process of new transfer learning classifier model is given as,

// Algorithm 2: New transfer learning classifier model

Input: Dataset, number of sensor nodes ' $sn_1, sn_2, sn_3, \ldots sn_n$', number of features ' $ft_1, ft_2, ft_3, \ldots ft_m$', weights '$We_k = We_1, We_2, We_3, \ldots . We_k$'

Output: Increase attack detection accuracy

Begin

1. **Collect n**umber of features and small number of sensor nodes--- **input layer**
2. **For each samples**
3. Choose relevant feature set
4. **End for**
5. **For each** training and testing samples
6. Measure similarity index
7. Obtain the multiple classification results
8. **End for**
9. **For every classification results**
10. Measure error rate
11. Update weights
12. **End for**
13. Initialize the population of the weights
14. **for each w**eight 'We_k'
15. Compute the fitness
16. **While ($t < t_{max}$) do**
17. Update the fish position
18. ***if*** $\left(f(F_i) > f(F_j)\right)$ **then**
19. It is considered as optimal weight
20. **else**
21. It is considered as non-optimal weight

22. End if

23. $t = t + 1$

24. End While

25. Obtain the final multi-stage classification results **at output layer**

26. End

Algorithm 2 describes the novel transfer learning model for accurate attack detection in wireless network with minimal error rate. For every data sample, weights and biases are allocated to the input layer. The input data is transmitted to the hidden layers where significant features are chosen doe minimizing the dimensionality. Then, the classification is performed to enhance attack detection accuracy. After the classification process, fine-tuning phase is performed using artificial fish swarm optimization. Initially, weights are determined. The fitness computed depending on error value and their positions are updated iteratively. This process gets repeated until maximum number of iteration is reached. Finally, artificial fish swarm optimization algorithm finds the optimal weight with lesser classification error. By this way, the attack detection is carried out in the wireless network. After attack detection, the secured data transmission is carried out using Signcryption technique.

3.4 Lamport Signcryption based Security Enhancement

Lamport Signcryption is considered as the public-key cryptography. The public key cryptography performed encryption and digital signature simultaneously. Lamport Signcryption in BKRSIDHTLN Method is used for performing security and data confidentiality enhancement. Lamport Signcryption performed three steps, namely key generation, signcryption, and unsigncryption.

- **Key Generation**

In key generation process, the base station generates private and public keys for eevery sensor node. By using the Lamport one-time signature, the private and public keys are created with help of one-way function. Let us consider that random positive integers as passwords. The password gets expired when the time get lapsed. It is given as,

$$Private\ key = [RI] \tag{13}$$

From (13), 'RI' denotes the random integer. After private key generation, the public verification key is generated as,

$$Public\ key = f[RI] \qquad (14)$$

From (14), 'f' represent the one-way function. It is formulated as,

$$f = [RI] + 1\ mod\ 16 \qquad (15)$$

The public verification keys are transmitted and the node private key is maintained secret.

- **Encryption and Signature Generation**

Lamport Signcryption is used to perform digital signature and encryption. Encryption and digital signature are considered as the cryptographic steps for improving the data confidentiality during data transmission between the sender node and base station in wireless networks.

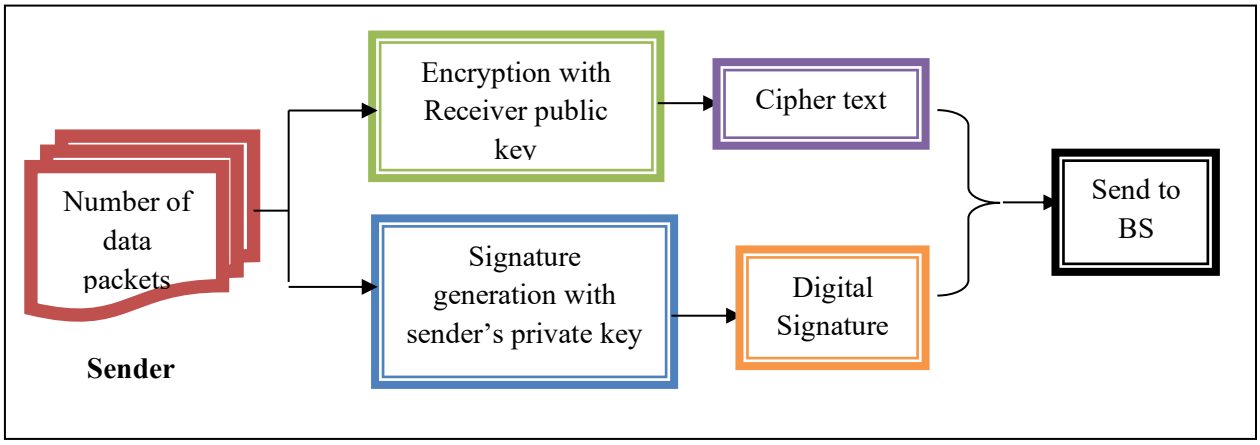


Figure 2 Signcryption Process

Figure 2 illustrates the signcryption process for increasing the data confidentiality and privacy during the data transmission between sensor nodes and base station through eliminating the unauthorized attacks. The sensed data packets '$dp_1, dp_2, .., dp_m$' are encrypted with receiver public key. The data packets are converted to the ciphertext. It is formulated as,

$$CT \leftarrow E\ [public\ key, dp] \qquad (16)$$

From (16), 'D' symbolizes the ciphertext of the data packets 'dp'. 'E' symbolizes the encryption with public key of receiver. At the same time, the digital signature is obtained with help of sender's private key. Let us consider that the 'z' as the positive integer. The positive integer is converted into string i.e., (0, 1) and digital signature is generated as,

$$\delta = [P_{ij\,z}] \qquad (17)$$

From (17), 'δ' symbolizes the signature. 'R_{ij}' represent the position of private key ranges from 0 to r. 'r' symbolizes the positive integer '$j \in (0,1)$'. The generated signature and cipher text is transmitted to the base station.

- **Unsigncryption**

The BKRSIDHTLN Method performs the unsigncryption (i.e., signature verification and decryption) to obtain the original data. Unsigncryption is the method of inversing the signcryption operation for decrypting the ciphertext and validating the signature to obtain the original image.

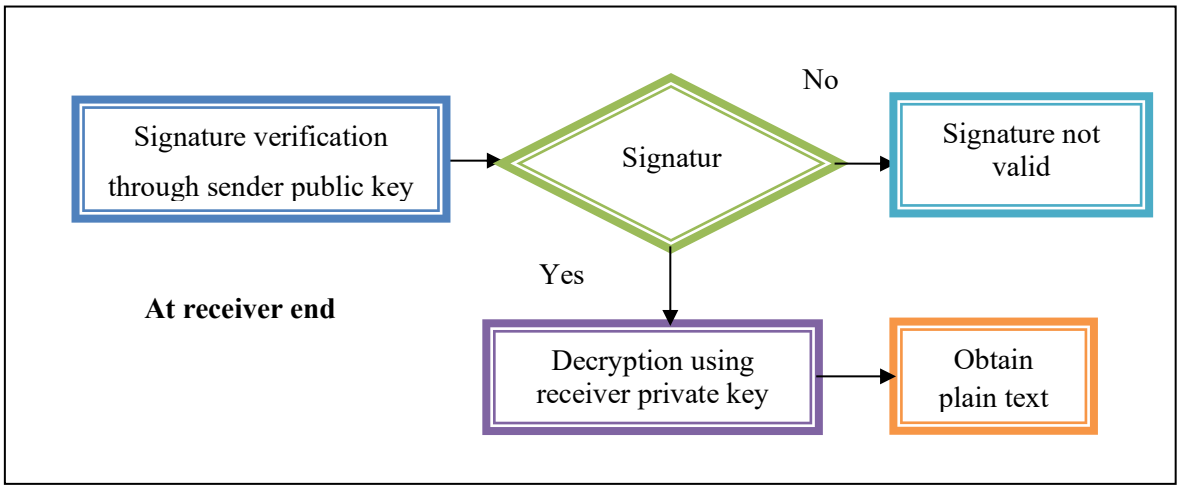


Figure 3 Unsigncryption Process

Figure 3 illustrates block diagram of unsigcryption process at the receiver end side. Initially, the signature verification is performed through the sender public key to attain the original data. It is formulated as,

$$\delta_b = f(\delta) \qquad (18)$$

$$f = [\delta] + 1 \; mod \; 16 \qquad (19)$$

From (19), 'δ_b' symbolizes the signature generated at the receiver side. 'f' represent the one-way function. Lastly, the signature is verified to obtain the original data.

$$Verification = \begin{cases} \delta = \delta_b & ; signature\ is\ valid \\ \delta \neq \delta_b & ; signature\ is\ not\ valid \end{cases} \quad (20)$$

When both signatures get matched, the base station decrypts the ciphertext to obtain the original data. Or else, the signature is not valid. The process improves the data transmission security between the sensor node and base station. Lastly, the authorized node (i.e., base station) decrypts the ciphertext and attained the plain data. It is formulated as,

$$d \leftarrow B[private\ key, D] \quad (21)$$

From (21), 'd' symbolizes the original data. 'B' represent the decryption. 'D' symbolizes the ciphertext. Lastly, the original data is attained at the base station. Finally, the secured data transmission is carried out with higher data confidentiality. The algorithmic process of the proposed technique is described as given below,

// Algorithm 3 Lamport Signcryption based Security Enhancement
Input: Number of data packets, Number of authorized sensor nodes **Output:** Increase the security of data transmission
Begin **1. Collect** the number of authorized sensor nodes 2. **for each** authorized sensor node **3.** Generate private and public key **9. End for** **<u>Signcryption</u>** **10** Encrypt data packets using receivers public key 11. Generate digital signature 12. Send cipher text and digital signature to the receiver **<u>Unigncryption</u>** 13. **for each** signature 14. Reconstruct the signature **15. End for**

16. **If** $(Generated\ signature = received\ signature)$ **then**
17. Signature valid
18. **else**
19. Signature is not valid
20. **End if**
21. **If** signature valid **then**
22. Receiver decrypt the cipher text
23. **End if**
24. **End**

Algorithm 3 illustrates the step-by-step process of secured data transmission between sensor node and base station. Initially, the input layer collects the number of data packets from the sender. Every sensor node gets registered by the base station and keys namely private and public keys are generated before data transmission. After key generation process, signcryption process is executed through encryption and signature generation with help of receiver's public key and the sender's private key. Then, the resulting cipher text and signature are sent to the receiver. The unsigncryption process is carried out through signature verification using sender's public key. When the signature is valid, the sensor node considered is authorized user. After that, the decryption process is carried out to obtain the plain text. Lastly, secured data transmission is carried out from sender to base station.

5. EXPERIMENTAL SETTINGS

Experimental evaluations of the proposed BKRSIDHTLN Method and existing methods namely machine learning-based selective attack mitigation model [1] and CL2ES methodology [2] are implemented using python language. The dataset used is UNSW-NB 15 dataset from https://research.unsw.edu.au/projects/unsw-nb15-dataset. To conduct the experiment, the UNSW-NB 15 is employed for distinguishing between normal and attacks. The last two columns in the datasets denote the category and label of data sample.

5. PERFORMANCE RESULTS AND COMPARISONS

In this section, performance analysis of the proposed BKRSIDHTLN Method and existing methods namely machine learning-based selective attack mitigation model [1] and CL2ES

methodology [2] are analyzed using various parameters, including attack detection accuracy, data confidentiality rate, data integrity rate, error rate and attack detection time. The results are given through table and graphical representations.

5.1 Performance of Attack Detection Accuracy

Attack detection accuracy is defined as the ratio of number of sensor nodes that correctly categorized as attacks or normal to total number of sensor nodes. Attack detection accuracy is computed as,

$$ADA = \left(\frac{T_p + T_n}{T_p + F_p + T_n + F_n}\right) * 100 \quad (22)$$

From (22), 'ADA' indicates attack detection accuracy, ' T_p' point outs a true positive, 'F_p' point outs a false positive, ' T_n' refers a true negative, 'F_n' refers a negative. It is calculated in terms of percentage (%).

Table 2 Comparison of Attack detection accuracy

Number of data samples	Attack detection accuracy (%)		
	Proposed BKRSIDHTLN Method	Machine learning-based selective attack mitigation model [1]	CL2ES methodology [2]
10000	97.2	94.1	93.2
20000	97.5	94.7	93.3
30000	98.9	94.5	93.4
40000	98.2	95.2	93.8
50000	98.6	94.5	93.9
60000	98.1	93.8	92.8
70000	98.3	94.7	93.7
80000	97.2	95.4	94.5
90000	98.5	94.1	93.8
100000	98.1	95.7	93.1

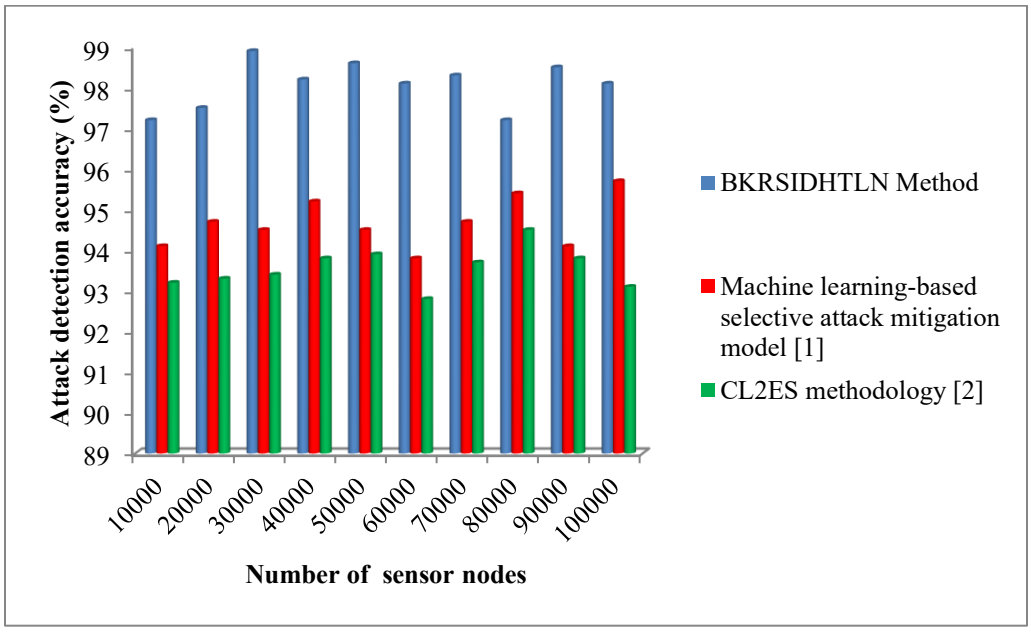


Figure 4 Analysis on Attack Detection Accuracy

Figure 4 shows the performance analysis of attack detection accuracy based on the number of sensor nodes. The attack detection accuracy using proposed BKRSIDHTLN Method is evaluated with two existing methods, namely Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2]. From above figure, '*X*' axis represents the number of sensor nodes and '*Y*' axis symbolizes the attack detection accuracy for three different techniques. The proposed BKRSIDHTLN Method increases the attack detection accuracy when compared to other existing techniques. In experiments conducted with 10000 data samples, the attack detection accuracy is 97.2%, 94.1% and 93.2% using BKRSIDHTLN method, Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2]. The enhancement is due to the application of Bayesian Kriging Regression analysis for choosing the relevant features to perform the attack detection. Zijdenbos similarity index is used in BKRSIDHTLN method for finding the data samples of selected features with testing data points for cyber attack detection. Generally, attack detection accuracy of proposed BKRSIDHTLN Method gets increased by 4% and 5% when compared to methods [1] and [2] respectively.

5.2 Performance of Data Confidentiality Rate:

Data confidentiality rate is defined as the ratio of the number of data packets received by authorized users to the number of data packets transmitted over the communication channel. It is formulated as,

$$DCR = \sum_{i=1}^{n} \left[\frac{DPAU}{ND_i}\right] * 100 \quad (23)$$

From (23), 'DCR' symbolizes the data confidentiality rate. 'ND_i' indicates the number of data packets. '$DPAU$' symbolizes the number of data packets received by authorized user. It is measured in percentage (%).

Table 3 Comparison of Data confidentiality rate

Number of data samples	Data confidentiality rate (%)		
	Proposed BKRSIDHTLN Method	**Machine learning-based selective attack mitigation model [1]**	**CL2ES methodology [2]**
10000	99.7	96.5	93.2
20000	99.8	96.7	94.1
30000	99.1	95.4	93.5
40000	99.5	95.6	94.6
50000	99.8	96.7	95.1
60000	99.4	95.7	94.8
70000	99.4	96.9	95.4
80000	99.3	95.7	94.9
90000	99.1	96.2	94.5
100000	99.7	94.25	93.4

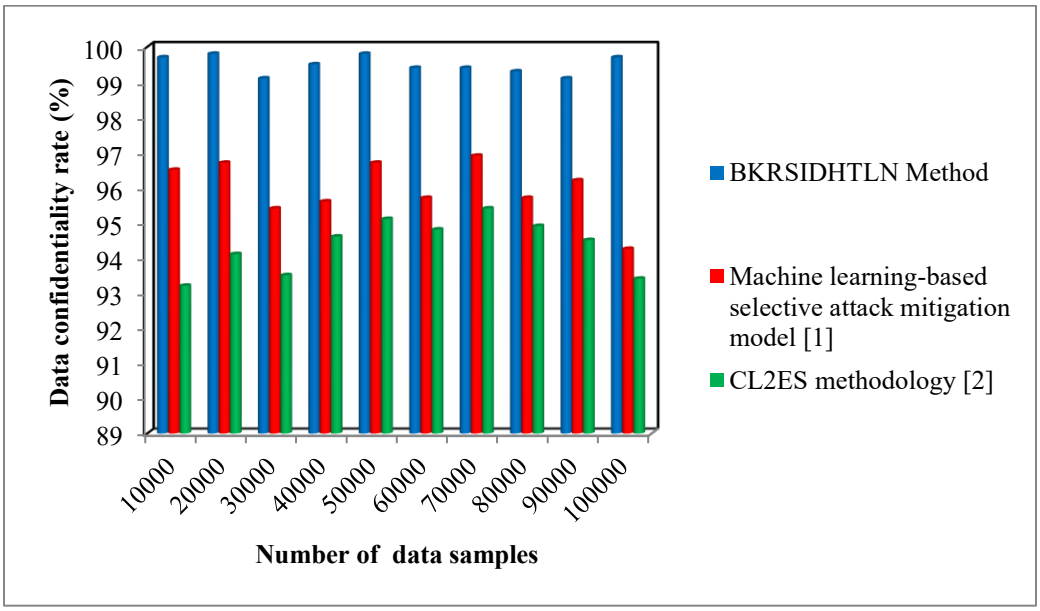


Figure 5 Analysis on Data Confidentiality Rate

Figure 5 illustrates the performance analysis of data confidentiality rate based on data samples gathered from input dataset. The data confidentiality rate using proposed BKRSIDHTLN Method is computed and compared with existing Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2]. From above figure, '*X*' axis symbolizes the number of data samples and '*Y*' axis represents the data confidentiality rate for three different techniques. Overall performance outcome indicates that the BKRSIDHTLN Method improves the data confidentiality rate when compared to other existing techniques. This improvement is achieved by Lamport Signcryption in BKRSIDHTLN Method for securely transmitting the normal data samples. The sender encrypts the data sample using the recipient's public key to promise confidentiality and generate the signature their own private key to guarantee the integrity. The receiver confirms the signature using the sender's public key and decrypts ciphertext using their private key for obtaining the original data. By this way, the secured data transmission is carried out in wireless networks. The data confidentiality rate of BKRSIDHTLN Method is improved by 4% and 5% when compared to existing Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2] respectively.

5.3 Performance of Data Integrity rate:

Data integrity rate is determined by the ratio of the number of data packets that remain unmodified or unaltered by unauthorized users to the total number of data packets transmitted over the communication channel. It is formulated as,

$$DIR = \sum_{i=1}^{n} \left[\frac{DPUA}{NDP}\right] * 100 \quad (24)$$

From (24), 'DIR' symbolizes the data integrity rate. 'NDP' indicates number of data packets. '$NPUA$' denotes the number of data packets unaltered. It is measured in percentage (%).

Table 4 Comparison of Data integrity rate

Number of data samples	Data integrity rate (%)		
	Proposed BKRSIDHTLN Method	**Machine learning-based selective attack mitigation model [1]**	**CL2ES methodology [2]**
10000	98.8	94.2	92.8
20000	99.5	94.7	92.7
30000	99.4	94.3	92.9
40000	99.2	94.5	92.8
50000	99.7	93.8	92.4
60000	99.4	93.6	93.4
70000	98.4	94.5	91.7
80000	98.8	94.7	92.8
90000	99.4	94.2	92.9
100000	99.	94.6	93.5

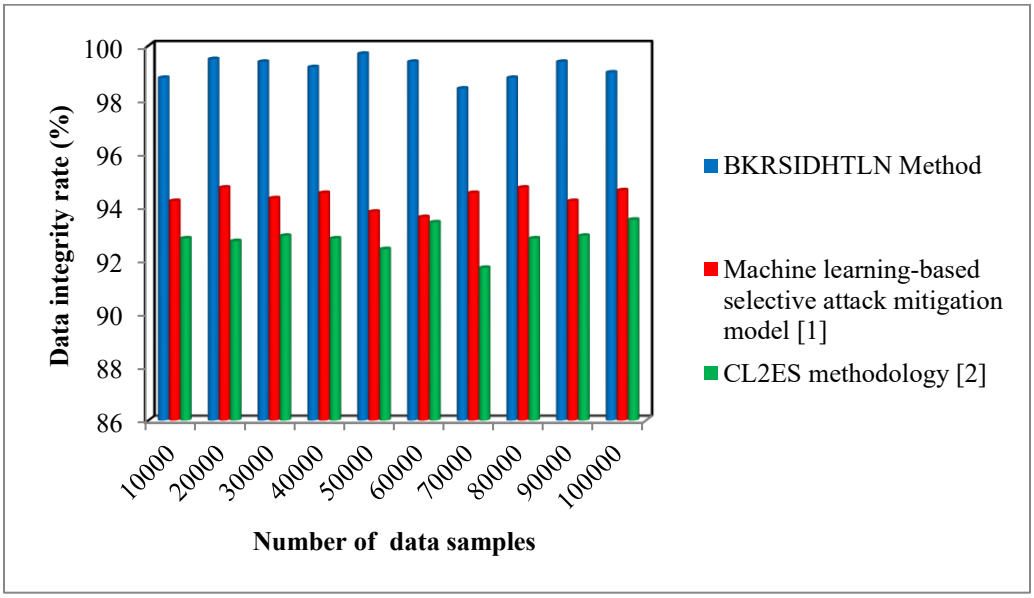


Figure 6 Analysis on Data Integrity Rate

Figure 6 illustrates the performance analysis of data integrity rate based on the data samples collected from input dataset. The data integrity rate using proposed BKRSIDHTLN Method is compared with existing Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2]. From above figure, '*X*' axis represents the number of data samples and '*Y*' axis symbolizes the data integrity rate for three different techniques. The proposed BKRSIDHTLN Method improves the data integrity rate when compared to other existing techniques. This enhancement is attained by Lamport Signcryption in BKRSIDHTLN Method for transmitting the normal data samples in secured manner. The sender encrypts the data sample using the recipient's public key to promise integrity and generate the signature own private key. The receiver verifies the signature by sender's public key and decrypts the ciphertext using their private key for attaining the original data. This in turn, the secured data transmission is carried out with higher integrity in wireless networks. The data integrity rate of BKRSIDHTLN Method is improved by 5% and 7% when compared to existing Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2] respectively.

5.4 Performance of attack detection time

Attack detection time is defined as the amount of time consumed for performing attack detection. It is calculated as follows,

$$ADT = \sum_{j=1}^{m} Ds_i * TM\ \ [CDs] \qquad (25)$$

From (25), 'ADT' indicates the attack detection time. '$TM[CDS]$' indicates a time for classifying single data packets 'Dp'. The time is measured in terms of milliseconds (ms). Lesser time consumption, the method is said to be more efficient.

Table 5 Comparison of Attack detection time

Number of data samples	Attack detection time (ms)		
	Proposed BKRSIDHTLN Method	**Machine learning-based selective attack mitigation model [1]**	**CL2ES methodology [2]**
10000	29	35	42
+920000	36	48	51
30000	50	56	65
40000	59	65	74
50000	70	81	82
60000	78	88	95
70000	85	96	104
80000	92	103	118
90000	101	110	125
100000	110	118	136

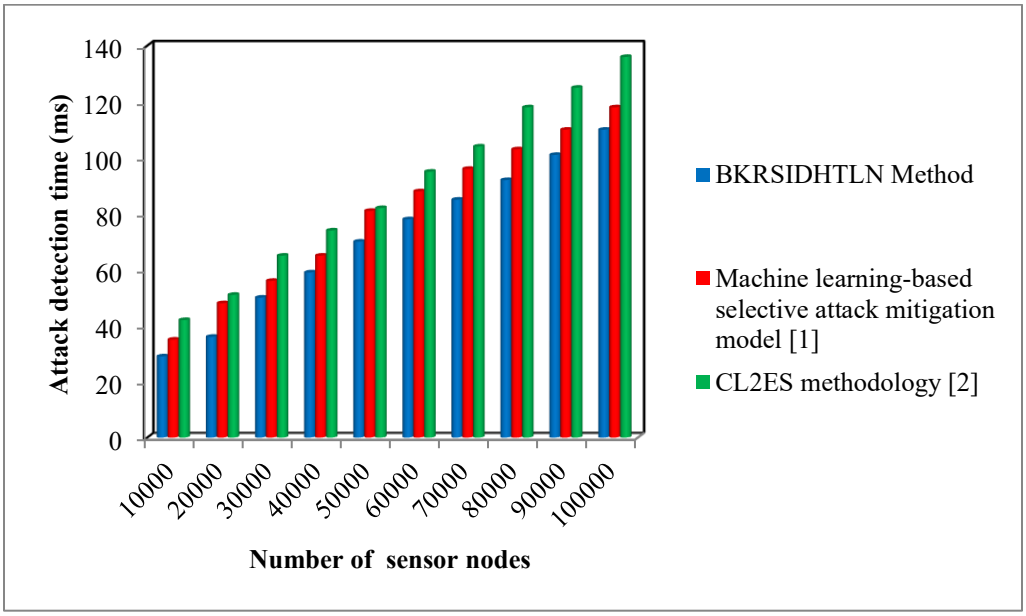


Figure 7 Analysis on Attack Detection Time

Figure 7 shows the performance analysis of attack detection time based on the number of sensor nodes gathered from the input dataset. The attack detection time using proposed BKRSIDHTLN Method is evaluated with existing Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2]. From above figure, '*X*' axis represents the number of sensor nodes and '*Y*' axis symbolizes the attack detection time for three different techniques. The proposed BKRSIDHTLN Method reduces the attack detection time when compared to other existing techniques. In experiments conducted with 10000 data samples, the time consumed for attack detection is 29ms, 35ms and 42ms using BKRSIDHTLN method, Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2]. The enhancement is due to the application of Bayesian Kriging Regression analysis to select the more relevant features from input dataset for performing attack detection. Zijdenbos similarity index is used in BKRSIDHTLN method for examining the data samples of selected features with testing data points for the cyber attack detection. Normally, attack detection time of BKRSIDHTLN method reduces attack detection time by 12% and 21% when compared to methods [1] and [2] respectively.

5.5 Performance of Error rate

Error rate is defined as the ratio of number of sensor nodes that incorrectly categorized as attacks or normal to total number of sensor nodes. Error rate is computed as,

$$ER = \left(\frac{F_p + F_n}{T_p + F_p + T_n + F_n}\right) * 100 \quad (26)$$

From (26), 'ER' indicates error rate, ' T_p' symbolizes true positive, 'F_p' represents false positive, ' T_n' denotes true negative, 'F_n' refers a negative. It is calculated in terms of percentage (%). Lesser the error rate, the method is said to be more efficient.

Table 6 Tabulation of Error Rate

Number of data samples	Attack detection accuracy (%)		
	Proposed BKRSIDHTLN Method	**Machine learning-based selective attack mitigation model [1]**	**CL2ES methodology [2]**
10000	2.8	5.9	6.8
20000	2.5	5.3	6.7
30000	1.1	5.5	6.6
40000	1.8	4.8	6.2
50000	1.4	5.5	6.1
60000	1.9	6.2	7.2
70000	1.7	5.3	6.3
80000	2.8	4.6	5.5
90000	1.5	5.9	6.2
100000	1.9	4.3	6.9

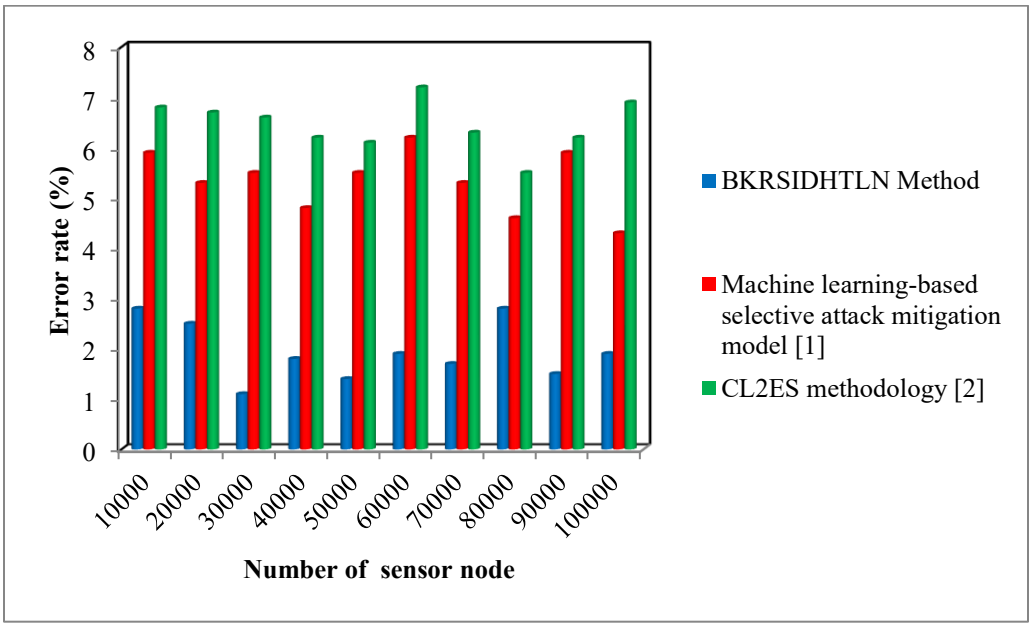


Figure 8 Analysis on Error Rate

Figure 8 shows the performance analysis of error rate based on the number of sensor nodes. The error rate using proposed BKRSIDHTLN Method is determined with two existing methods, namely Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2]. From above figure, '*X*' axis symbolizes the number of sensor nodes and '*Y*' axis symbolizes the error rate for three different methods. The proposed BKRSIDHTLN Method reduces the error rate when compared to other existing techniques. In experiments conducted with 10000 data samples, the error rate is 2.8%, 5.9% and 6.8% using BKRSIDHTLN method, Machine learning-based selective attack mitigation model [1] and CL2ES methodology [2]. The enhancement is because of using Bayesian Kriging Regression analysis to select relevant features for attack detection. Zijdenbos similarity index identified the normal data samples of selected features with testing data points for efficient cyber attack detection. This in turn, BKRSIDHTLN Method reduces the error rate. Subsequently, error rate of proposed BKRSIDHTLN Method gets reduced by 63% and 70% when compared to methods [1] and [2] respectively.

6. CONCLUSION

In this paper, a new secure data transmission technique called Bayesian Kriging Regressive Similarity Index Deep Highway Transfer Learning Network (BKRSIDHTLN) Method is introduced. The designed method performed two processes, namely attack detection and secure transmission technique. Bayesian Kriging Regression analysis chooses the more relevant features

for efficient attack detection. Zijdenbos similarity index examines the data samples of selected features for cyber attack detection. With the similarity value, data sample is categorized into normal and attack nodes. Lamport Signcryption in BKRSIDHTLN Method securely transmits the normal data samples. The sender encrypts the data sample through recipient public key to improve the confidentiality and generate signature with own private key to guarantee integrity. The recipient confirms the signature using the sender's public key and then decrypts the ciphertext using their private key to get the original data. By this way, the secured data transmission is carried out in wireless networks. The obtained results confirm that the BKRSIDHTLN Method increases the attack detection accuracy, data confidentiality, integrity with minimal time and error rate than the state-of-the-art methods.

REFERENCES

[1] Talal Albalawi and P. Ganeshkumar, "CL2ES-KDBC: A Novel Covariance Embedded Selection Based on Kernel Distributed Bayes Classifier for Detection of Cyber-Attacks in IoT Systems", Computers, Materials and Continua, Elsevier, Volume 78, Issue 3, 26 March 2024, Pages 3511-3528

[2] Soyoung Joo, So-Hyun Park, Hye-Yeon Shim, Ye-Sol Oh and Il-Gu Lee, "Machine Learning-Based Detection and Selective Mitigation of Denial-of-Service Attacks in Wireless Sensor Networks", Computers, Materials and Continua, Elsevier, Volume 82, Issue 2, 17 February 2025, Pages 2475-2494

[3] Ayuba John, Ismail Fauzi Bin Isnin, Syed Hamid Hussain Madni and Muhammed Faheem, "Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms", Intelligent Systems with Applications, Elsevier, Volume 22, June 2024, Pages 1-15

[4] Olivia Jullian, Beatriz Otero, Eva Rodriguez, Norma Gutierrez, Hector Antona and Ramon Canal, "Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack

Detection Framework", Journal of Network and Systems Management, Springer, Volume 31, Issue 33, 2023, Pages 1-15

[5] Revathi Subramaniam, Androse Joseph Sheela and Abdullah Alwabli, "Enhanced cybersecurity and cyber-attack detection in smart DC micro grids using blockchain technology and SVM technique", Ain Shams Engineering Journal, Elsevier, Volume 16, Issue 7, July 2025, Pages 1-15

[6] Sultan Refa Alotaibi, Fatma S. Alrayes, Wahida Mansouri, Hamed Alqahtani, Samah Hazzaa Alajmani, Moneerah Alotaibi, Fouad Shoie Alallah and Abdulrhman Alshareef, "An ensemble of fuzzy soft expert set with deep learning on attack detection for secure industrial cyber-physical systems", Journal of Radiation Research and Applied Sciences, Elsevier, Volume 18, Issue 2, June 2025, Pages 1-15

[7] Roberto Canonico, Giovanni Esposito, Annalisa Navarro, Simon Pietro Romano, Giancarlo Sperli and Andrea Vignali, "An anomaly-based approach for cyber–physical threat detection using network and sensor data", Computer Communications, Elsevier, Volume 234, 15 March 2025, Pages 1-15

[8] Abdullah Alabdulatif, Navod Neranjan Thilakarathne and Mohamed Aashiq, "Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System", Computers, Materials and Continua, Elsevier, Volume 80, Issue 3, 12 September 2024, Pages 3655-3683

[9] Muneeswari G., Mabel Rose R.A., Balaganesh S., Jerald Prasath G., and Chellam S. "Mitigation of attack detection via multi-stage cyber intelligence technique in smart grid", Measurement: Sensors, Elsevier, Volume 33, June 2024, Pages 1-15

[10] Gebrekiros Gebreyesus Gebremariam, J. Panda and S. Indu, "Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models", Alexandria Engineering Journal, Elsevier, Volume 82, 1 November 2023, Pages 82-100

[11] P. Sathishkumar, A. Gnanabaskaran, M. Saradha and R. Gopinath, "Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network", Ain Shams Engineering Journal, Elsevier, Volume 15, Issue 12, December 2024, Pages 1-15

[12] K. Sedhuramalingam and N. Saravanakumar, “A novel optimal deep learning approach for designing intrusion detection system in wireless sensor networks”, Egyptian Informatics Journal, Elsevier, Volume 27, September 2024, Pages 1-15

[13] Muawia A. Elsadig., “Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach”, EEE Access, Volume 11, August 2023, Pages 83537 – 83552

[14] Vikash Kumar Singh, Durga Sivashankar, Kishlay Kundan and Sushmita Kumari, “An Efficient Intrusion Detection and Prevention System for DDOS Attack in WSN Using SS-LSACNN and TCSLR”, Journal of Cyber Security and Mobility, Volume 13, Issue 1, January 2024, Pages 135 – 159

[15] Julian Karoliny, Bernhard Etzlinger, Roya Khanzadeh, Andreas Springer and Hans-Peter Bernhard., “Network Support Layers Trustworthiness Computation for Wireless Networks”, IEEE Transactions on Communications, Volume 73, Issue 3, March 2025, Pages 1879 – 1894

[16] Chen Quan, Nandan Sriranga, Haodong Yang, Yunghsiang S. Han Baocheng Geng and Pramod K. Varshney, “Efficient Ordered-Transmission Based Distributed Detection under Data Falsification Attacks”, IEEE Signal Processing Letters, Volume 30, February 2023, Pages 145 – 149

[17] Rana Al-Rawashdeh, Ahmed Aljughaiman, Abdullah Albuali, Yousef Alsenani and Mohammed Alnaeem, “Enhancing DoS Detection in WSNs Using Enhanced Ant Colony Optimization Algorithm”, IEEE Access, Volume 12, September 2024, Pages 134651 – 134671

[18] Halima Sadia; Saima Farhan; Yasin Ul Haq; Rabia Sana; Tariq Mahmood; Saeed Ali Omer Bahaj, “Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach”, IEEE Access, Volume 12, March 2024, Pages 52565 – 52582

[19] Wei Xie, Hongjun Wang, Zimo Feng and Chunlai Ma, “A Novel PHY-Layer Spoofing Attack Detection Scheme Based on WGAN-Encoder Model”, IEEE Transactions on Information Forensics and Security, Volume 19, September 2024, Pages 8616 - 8629

[20] Weibin Jiang, Jun Wang, Kan-Lin Hsiung and Hsin-Yu Chen, "GRNN-Based Detection of Eavesdropping Attacks in SWIPT-Enabled Smart Grid Wireless Sensor Networks", IEEE Internet of Things Journal, Volume 11, Issue 22, 15 November 2024, Pages 37381 – 37393

[21] Anila Kousar, Saeed Ahmed, Abdullah Altamimi, Su Min Kim and Zafar A. Khan, "Stealthy data integrity attack identification in smart grid networks utilizing deep denoising autoencoder", Heliyon, Elsevier, Volume 10, Issue 19, 15 October 2024, Pages 1-18

[22] Sultan H. Almotiri, "Improving network resilience against DDoS attacks: A fuzzy TOPSIS-based quantitative assessment approach", Heliyon, Elsevier, Volume 10, Issue 22, 30 November 2024, Pages 1-15

[23] Yangrong Chen, June Li, Yu Xia, Ruiwen Zhang, Lingling Li, Xiaoyu Li and Lin Ge, "Fortifying Smart Grids: A Holistic Assessment Strategy against Cyber Attacks and Physical Threats for Intelligent Electronic Devices", Computers, Materials and Continua, Elsevier, Volume 80, Issue 2, 15 August 2024, Pages 2579-2609

[24] Muhammad Akbar Husnoo, Adnan Anwar, Haftu Tasew Reda, Nasser Hosseinzadeh, Shama Naz Islam, Abdun Naser Mahmood and Robin Doss, "FedDiSC: A computation-efficient federated learning framework for power systems disturbance and cyber attack discrimination", Energy and AI, Elsevier, Volume 14, October 2023, Pages 1-15

[25] Jawad Hassan, Adnan Sohail, Ali Ismail Awad and M. Ahmed Zaka, "LETM-IoT: A lightweight and efficient trust mechanism for Sybil attacks in Internet of Things networks", Ad Hoc Networks, Elsevier, Volume 163, 1 October 2024, Pages 1-15

[26] Shaymaa Mahmood Naser, Yossra Hussain Ali and Dhiya Al-Jumeily, "Hybrid Cyber-Security Model for Attacks Detection Based on Deep and Machine Learning", International Journal of Online and Biomedical Engineering (iJOE), Volume 18, Issue 11, August 2022, Pages 17-30

[27] Ahmed Bensaoud and Jugal Kalita, "Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models", Ad Hoc Networks, Elsevier, Volume 170, April 2025, Pages 1-18

[28] Dr S Malathi and S. Razool Begum, “Enhancing trustworthiness among IoT network nodes with ensemble deep learning-based cyber attack detection”, Expert Systems with Applications, Elsevier, Volume 255, Part A, 1 December 2024, Pages 1-15

[29] Uras Panahi and Cuneyt Bayilmis, “Enabling secure data transmission for wireless sensor networks based IoT applications”, Ain Shams Engineering Journal, Elsevier, Volume 14, Issue 2, March 2023, Pages 1-15

[30] M. Joselin Kavitha, M.R. Geetha and R. Isaac Sajan, “Knowledge-based adaptive routing for energy efficiency and attack detection in ad hoc wireless sensor networks”, Computer Networks, Elsevier, Volume 259, March 2025, Pages 1-15