Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

Probabilistic Deming Deep Recursive Network and Schmidt-Samoa Cryptosystem for Cyber Attack Detection and Secure Transmission in Wireless Networks

[1]Dhivya. R , [2] Dr. B. Srinivasan

[1]PHD Part Time, Department Of Computer Science, Gobi Arts & Science College, Karattatipalayam, Gobichettipalaym, Erode (DT).

[2]Associate Professor,Department Of Computer Science,Gobi Arts & Science college,Karattatipalayam,Gobichettipalaym, Erode (DT).

Article History:

Received: 12-01-2025

Revised: 15-02-2025

Accepted: 01-03-2025

Abstract:

A wireless network is an elastic data communications system that exploits wireless media to broadcast data over the network. In wireless network, cyber attack detection is vital for maintaining the security and integrity of communication systems since these networks are more susceptible to different threats due to their open, dynamic, and broadcast nature. Therefore, cyber-attacks are becoming more difficult, targeting systems that handle or store sensitive information. Due to the rapid increase in cyber-attacks, the design of a detection mechanism discovers the harmful effect and attacks. The developed mechanisms for cyber attack detection unable to achieve higher detection accuracy and security in the data transmission. Therefore, a novel method referred as Probabilistic Deming Regressive Deep Recursive Network based Kupyna Schmidt-Samoa Signcryption (PDRDRN-KSSS) technique is proposed for efficient cyber attack detection in wireless network with better accuracy and security. PDRDRN-KSSS performs two different processes such as classification and secure data transmission. The classification is performed using Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network for cyber attack detection. The designed network obtains number of data samples and their features as input. Then, the feature selection is performed using Deming Regression analysis to choose the more relevant features from the dataset for attack detection. After that, the cyber attacks detection is performed through classifying the data samples with selected feature using the Tversky Similarity Index. Tversky Similarity Index is used to analyze the training data and mean of the particular classes. Based on similarity value, data samples are classified into normal and different types of attack nodes (i.e., Fuzzers node, Analysis node, Backdoors node, DoS node, Exploits node, Generic node and Reconnaissance node). Followed by this, the Cramer's correlated Kupyna Schmidt-Samoa Signcryption is used for securely transmit 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. 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 ciphertext and the signature are sent to the recipient. 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. With this, secure data transmission is achieved in wireless networks. Experimental evaluation is carried out on metrics such as data confidentiality rate, integrity rate, attack detection accuracy and attack detection time with respect to different number of data samples. The results confirm that the proposed PDRDRN-KSSS method attains better accuracy, integrity,

confidentiality with lesser time.

Keywords: Wireless network, Cyber Attack Detection**,** Secure Data Transmission, Deming Regressive, Kupyna Schmidt-Samoa Signcryption

1. Introduction

Cyber attack detection and secure data transmission are key steps to protect the wireless networks that are prone to a wide range of security threats. As wireless communication becomes more omnipresent, the threat of cyber attacks such as illegal access, eavesdropping, and data manipulation grows, posing important threats to the integrity, confidentiality, and availability of transmitted information. Efficient cyber attack detection involves examining network traffic to recognize distrustful activities while secure data transmission ensures that sensitive information remains protected from tampering. By leveraging encryption techniques, wireless networks diminish these risks, maintaining both the security and trustworthiness of communications in an ever-evolving digital landscape.

A Blockchain supported SDN based hybrid Moving Target Defense model was developed in [1] to detect the attack in the network. It integrated blockchain technology and Quantum Convolutional Neural Networks (QCNN) in the SDN environments. However, the confidentiality rate was not improved. Federated Learning based Multi-Party computation for intrusion detection systems (FBMP-IDS) was introduced in [2] to attain higher detection rate of attacks. The model minimizes the communication overhead and computational complexity. However, the data transmission was performed securely.

A blockchain based federated deep learning scheme was designed in [3] to securely forward the data in IoT networks. It protected the privacy of the data during the transmission. Though the scheme avoids the unauthorized access, data integrity was not addressed. A novel parallel-pipelined-memory (P^2M) Blowfish model was introduced in [4] for IoT networks. However, the accuracy of attack detection was not improved.

An adapted Convolutional Neural Network based IDS (CNN-IDS) scheme was developed in [5] to increase the efficacy of attack detection. However, the attack detection time was not minimized. Also, IDS through the transformer-based transfer learning was developed in [6] to find the attack in unfair network traffic. It examines the feature interactions in both network feature demonstration and imbalanced data. However, the security while transmitting the data was not attained efficiently.

A federated learning system based on Multi-Layer Perceptron was introduced in [7] to determine the IoT botnet attacks. XGBoost model was employed for pertinent feature selection and Principal Component Analysis was used for dimensionality minimization. With this, computational complexity was reduced. However, the efficiency of attack detection was not improved. A Federated Learning-based IDS (FL-IDS) was introduced in [8] to progress the security IoT network via increasing the data privacy. But, the time complexity was not reduced.

An Improved deep neural network (IDNN) was designed in [9] to perform anomaly intrusion detection in WSN. The global search strategy of the coyote optimization was applied to establish

network topologies. A blockchain-machine learning (BC-ML) was introduced in [10] improved malevolent node identification in WSN. However, the precision and recall rate was not increased sufficiently.

Evasion Generative Adversarial Network based on the deep reinforcement learning was introduced in [11] for botnet detection. However, robustness of the attack detection was not enhanced. A deep neural network-based IDS was discovered to recognize malevolent data in real-time. Accuracy was not enhanced. A Deep Neural Network based real-time IDS was presented in [12] for IoT to solve the diverse security threats. Machine learning based model was developed in [13] to discover the DoS attack in wireless network. Improved quantum neural network and elliptical curve cryptography was designed in [14] to determine the attacks for better data security. Modified Dwarf Mongoose optimization with deep learning was introduced in [15] to identify the attack detection.

1.1 Contribution

- A new PDRDRN-KSSS technique is developed for cyber attack detection based on the classification and secure data transmission process in wireless network with higher accuracy and data integrity rate.
- To accurately classify the data samples into normal or attacks, Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network is designed.
- To select pertinent features and eliminate the irrelevant features for attack detection, Probabilistic Deming Regression analysis is used in the deep recursive network that minimizes the time involved in the attack detection.
- To enhance the secure data transmission in wireless network in terms of higher data confidentiality and integrity, Cramer's correlated Kupyna Schmidt-Samoa Signcryption is designed to perform key generation, signcyption and unsigncyption.
- Finally, an experimental evaluation is conducted to compute the performance of the PDRDRN-KSSS technique using various metrics and compared to state-of-the-art methods.

1.2 Organization of paper

The paper is organized into the following sections: Section 2 reviews related work. Section 3 describes the PDRDRN-KSSS with a detailed diagram. Section 4 outlines the experimental settings and section 5 gives a comparative analysis of various metrics with different methods. Finally, Section 6 presents the overall conclusion.

2. Related works

A deep variational autoencoder (DVAE) classifier was applied to categorize the attack samples. DoS attack identification through the fuzzy temporal deep long Short-Term memory was carried out in [16] for WSN. By applying ML based E-shaped structure with algorithms, anomaly detection was performed in WSN [17]. To enhance the data security, improved elliptic key cryptography was developed in [18] for wireless network. Through combining the Deep Neural Networks and Convolutional Neural Network, the ability of IDS was enhanced in [19]. A probabilistic data

structures and Deep Learning techniques were designed in [20] to process traffic data for attack detection. The technique reduces the false alarm rate.

A lightweight machine learning detection model depended on the decision tree (DT) with the Gini feature selection method was developed in [21] to sense DoS attacks. An efficient deep learning based solution was provided by [22] to IDS in wireless network. Statistics and higher-order descriptors were employed to extract the features for attack detection. An intelligent hybrid model through deep and machine learning technologies for cyber attack detection in [23].The model increased cyber-attack detection speed. A novel deep learning model referred as Device-based Intrusion Detection System (DIDS) was designed in [24]. The designed model combines the prediction of anonymous attacks to solve computational overhead in large networks and increase the throughput with a low false alarm rate. The computational time was reduced and accuracy of attack detection was enhanced. A distributed approach depended on the deep learning (DL) to avoid several various sources of susceptibility at once all under the same protection system [25]. Two different DL models were a applied to find the different kinds of attacks. Federated deep belief network based wireless IDS system was developed in [26] to find the cyber attack. FL was employed to generate a global model. A hybrid machine and deep learning approach was introduced in [27] to improve IDS. XGBoost and CNN were applied for feature extraction and then integrates each of these with LSTM for classification. Performance evaluation of DL techniques for DoS attacks identification in wireless network was developed in [28]. An intelligent hybrid scheme was designed using ML and artificial intelligence to boost the security of WSNs through recognizing and preventing cyberattacks [29]. Optimized hybrid DL and improved encryption algorithm over IoT was developed in [30] for security development and attack detection.

3. Proposed Methodology

Currently, the extensive use of the Internet has made life more suitable for everyone but it has also made cyber security threats harder to combat. With the advent of IoT devices such as smart objects, smart handheld devices, and smart sensing technologies, it is now probable to process enormous amounts of data rapidly and efficiently. However, such systems are consequently prone to a wide range of malevolent attacks and security flaws. Traditional methods applied for identifying these attacks compromise data integrity and confidentiality. Therefore, novel attack detection and secure transmission technique called PDRDRN-KSSS is designed in wireless network.

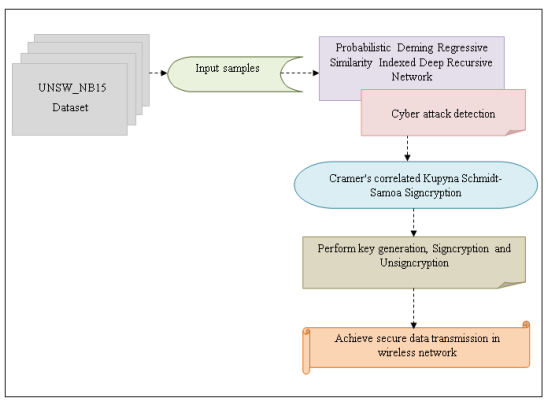

Figure 1 Architecture of proposed PDRDRN-KSSS technique

Figure 1 demonstrates the architecture of the proposed PDRDRN-KSSS technique for cyber attack detection secure data transmission in wireless network. Initially, number of data samples is gathered from the given database. Then, the Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network is employed to detect the attack in the network through the feature selection and data sample classification procedures. Afterward, Kupyna Schmidt-Samoa Signcryption is applied to securely transmit the data in wireless networks. This in turns, the integrity and confidentiality of the data increased. The above described PDRDRN-KSSS technique is briefly explained in following sections.

3.1 Data acquisition

The input data is used to attain the attack detection and secure transmission. The proposed PDRDRN-KSSS technique uses the UNSW-NB15 dataset. The dataset is collected from https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15. UNSW-NB15 includes certain standards dataset that contain many attacks that are simulated on network environment. The dataset encompasses 175,341 data samples with 45 features or attributes. The last two columns point outs the attack category and label for each sample data. The categories of attack types are fuzzers, analysis, backdoors, DoS, exploits, generic, reconnaissance, shellcode, worms attacks. The features of the dataset of UNSW-NB15 are given in Table 1.

Table 1: Features of UNSW-NB15 dataset

S.Count	Features	Category
1	dur	Float
2	proto	Categorical
3	service	Categorical
4	state	Categorical
5	spkts	Integer
6	dpkts	Integer
7	sbytes	Integer
8	dbytes	Integer
9	rate	Float
10	sttl	Integer
11	dttl	Integer
12	sload	Float
13	dload	Float
14	sloss	Integer
15	dloss	Integer
16	sinpkt	Float
17	dinpkt	Float
18	sjit	Float
19	djit	Float
20	swin	Integer

21	stcpb	Integer
22	dtcpb	Integer
23	dwin	Integer
24	tcprtt	Float
25	synack	Float
26	ackdat	Float
27	smean	Integer
28	dmean	Integer
29	trans_depth	Integer
30	response_body_len	Integer
31	ct_srv_src	Integer
32	ct_state_ttl	Integer
33	ct_dst_ltm	Integer
34	ct_src_dport_ltm	Integer
35	ct_dst_sport_ltm	Integer
36	ct_dst_src_ltm	Integer
37	is_ftp_login	Binary
38	ct_ftp_cmd	Integer
39	ct_fw_http_mthd	Integer
40	ct_src_ltm	Integer
41	ct_srv_dst	Integer
42	is_sm_ips_ports	Binary

3.2 Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network

Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network is applied upon acquiring the data samples for cyber attack detection. The recursive neural network is a category of deep learning architecture to examine the data samples with their features using several layers. A recursive neural network is build through the same set of weights recursively over a structured input for creating a structured prediction. Structure of Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network classifier is shown in Figure 2.

The designed network comprises one input layer, two hidden layers and one output layer. The sensor nodes are used to collect the distributed network data. The collected data are sent to the input layer of deep recursive learning model. After that, the collected input is sent to the hidden layer 1. In that layer, the feature selection process is performed using the Deming Regression analysis. The more pertinent features are considered for attack detection to diminish the time complexity. After that, the Cybersecurity attacks detection is performed through the classification in next hidden layer with the selected feature using the Tversky Similarity Index. Lastly, the classified output of normal data and different types of attacks are identified at an output layer of deep recursive classifier. From this, accurate attack detection is achieved in PDRDRN-KSSS technique.

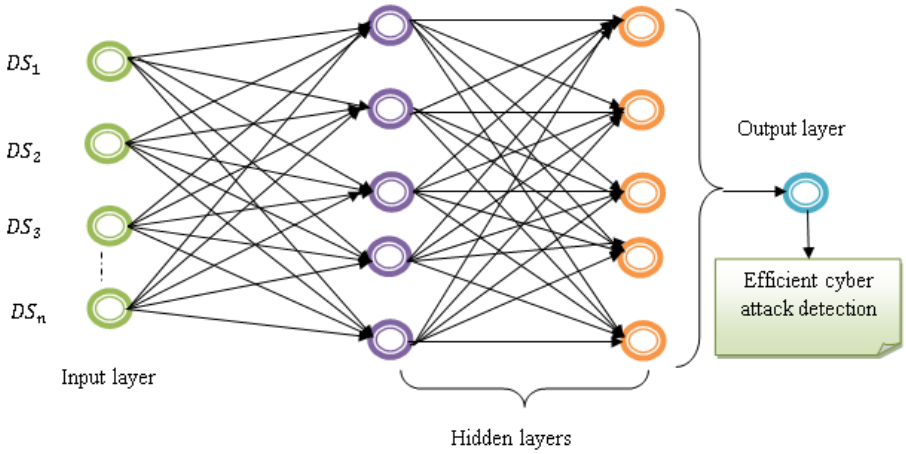

Figure 2 Structure of Recursive Deep Neural Network

Figure 2 illustrates the structure of Recursive Deep Neural Network to classify the data samples for accurate cyber attack detection. The neuron in one layer is associated to each neuron into another layer to build the whole network. The input layer obtains the data samples $\{DS_1, DS_2, DS_3, \ldots, DS_n\}$ as input from given dataset. Neuron activity in the input layer is formulated as follows.

$$p(t) = \sum_{i=1}^{n} DS_i * \delta + \vartheta \quad (1)$$

Where '$p(t)$' point outs the input layer, 'DS_i' point outs number of data samples, 'δ' point outs a weight between input and hidden layer and 'ϑ' refers a bias (generally taken as 1). The input is forwarded into the hidden layer one to carry out the feature selection process using Probabilistic Deming Regression model. By performing feature selection process, the dimensionality of the dataset is reduced and thereby minimizes the time complexity in the attack detection.

In PDRDRN-KSSS, probabilistic deming regression model is used for select the most relevant features among the number of features in the dataset. It is statistical model applied to compute the association between two variables such as independent (i.e., sample data features β) and dependent variable (i.e. outcomes Y). Here, the dependent variable takes two outcomes (i.e., pertinent or irrelevant). The objective of probabilistic deming regression model is to compute the relationship between features.

Consider the dataset includes number of data samples $\{DS_1, DS_2, DS_3, \ldots, DS_n\}$ and features $\{\beta_1, \beta_2, \beta_3, \ldots, \beta_f\}$. The designed deming regression takes available features (α_i, β_i) are predicted observations of the true values (α_i', β_i'), that lie on the regression line as formulated as given below.

$$\alpha_i = \alpha_i' + \gamma_i \quad (2)$$

$$\beta_i = \beta_i' + \varepsilon_i \quad (3)$$

In the above equations, 'γ_i' and 'ε_i' denotes the independent and the ratio of their variances is considered to be identified. To determine the intercept 'a_0' and the slope 'a_1' in the equation is expressed as follows.

$$\widehat{T_v} = c_0 + c_1\widehat{\beta_v} \quad (4)$$

In the above equation (4), '$\widehat{T_v}$' and '$\widehat{\beta_v}$' point outs the estimates of expected values of 'β_i' and 'α_i' respectively. Through the above equations, the best fit line for each feature is identified by the deming regression and thereby selects the relevant features for significantly finds the attack detection. Therefore, the pertinent features for attack detection are identified in hidden layer one. The selected features forwarded to the hidden layer two where the classification of data samples is made for attack detection. In that layer, Tversky similarity index is measured is applied to examine training data and mean of the particular classes.

Considers the number of classes $l_1, l_2, .. l_x$ and the mean $m_1, m_2 \ldots m_y$. Then the Tversky similarity index is used to compute the associate between the class mean and the extracted features. According to the similarity value, the sample data are classified into specific class.

$$\omega = \frac{E\beta_i \cap m_y}{g\left(E\beta_i \Delta m_y\right) + h\left(E\beta_i \cap m_y\right)} \quad (5)$$

In the above equation (5), 'ω' refers a Tversky similarity index coefficient, '$E\beta_i$' refers extracted features, 'm_y' refers a mean of class, '$E\beta_i \cap m_y$' refers a mutual dependence between the feature and mean of class, '$E\beta_i \Delta m_y$' indicates a variance between the extracted features and mean of class. Also, 'g' and 'h' refers a parameters of the Tversky index ($g, h \geq 0$). The similarity coefficient (ω) gives the value between [0, 1]. Thus, the output of Tversky similarity index is given as follows.

$$\omega = \begin{cases} 1 & data\ is\ classified\ as\ attack \\ 0 & data\ is\ classified\ as\ normal \end{cases} \quad (6)$$

In the above equation (6), Tversky similarity index 'ω' returns '1' as output when similarity between data with extracted features and mean value of the class are higher and the data is classified into different types of attacks. On the other hand, Tversky similarity index 'ω' returns '0' as output when similarity between data with extracted features and mean value of the class are lower and the data is classified into normal. Lastly, the output of classification is obtained at the output layer of deep recursive neural network. From this, accurate cyber attack detection is achieved with minimal time. Algorithm of Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network is described as follows.

Algorithm1: Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network
Input: Dataset 'D', data samples $DS_1, DS_2, DS_3, \ldots DS_n$ with features $\{\beta_1, \beta_2, \beta_3, \ldots., \beta_f\}$ **Output:** Cyber attack detection
Begin **1.** Take samples $DS_1, DS_2, DS_3, \ldots DS_n$ at an input layer **2.** **For each** data sample DS_i **3.** Assign weight and bias **4.** Formulate neuron activity in input layer '$p(t)$' **5.** **End for**

6. **For each** features
7. Perform Probabilistic Deming Regression // hidden layer one
8. Analyze relationship between features
9. Find best fit line
10. Extract more relevant features
11. **End for**
12. **For** each selected relevant feature with data samples DS_i
13. Perform Tversky similarity index using (5) // hidden layer two
14. **End for**
15. **if** $(\omega = 1)$ **then**
16. Data samples is classified as attack
17. **else**
18. Data samples is classified as normal
19. **End if**
20. **Return** classifications outcomes //output layer
21. **End for**

End

The above algorithm 1 shows the step by step process of probabilistic deming regressive similarity indexed deep recursive network for detecting the cyber attack in wireless network using feature selection and classification. At first, the input layer gets a number of data samples and features as input. Then, the input is given to the first hidden layer for choosing the relevant features from the dataset. This is done by applying the probabilistic deming regressive function where the relationship between the input features is determined. Then, the selected features are given to the second hidden layer to carry out the data classification. The second hidden layer utilizes Tversky similarity index to classify the data samples into normal and attacks. Lastly, the output layer provides predicted results of cyber attack detection. Thus, the probabilistic deming regressive similarity indexed deep recursive network gives better performance of cyber attack detection with lower time and higher accuracy.

3.3 Cramer's Correlated Kupyna Schmidt-Samoa Signcryption Model

Once the data is classified into normal and attack, the proposed PDRDRN-KSSS technique performs Kupyna Schmidt-Samoa Signcryption Model for secure data transmission. The Kupyna Schmidt-Samoa Signcryption Model is a cryptographic framework that combines both encryption and digital signature functions into a single operation for presenting more significant solution in the secure data transmission.

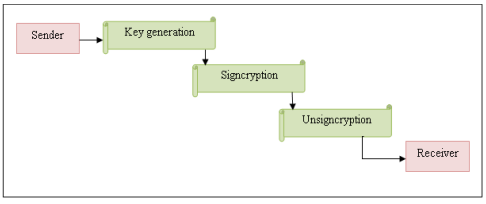

Figure 3 Cramer's correlation Kupyna Schmidt-Samoa Signcryption Model

As given in the above figure 3, Cramer's correlated Kupyna Schmidt-Samoa Signcryption model includes three processes namely key generation, Signcryption, and Unsigncryption to securely transmit the normal data samples. Through integrating the Kupyna encryption algorithm with Schmidt-Samoa's signcryption approach, the model guarantees both the confidentiality and authenticity of the data. Also with this Signcryption model, computational complexity and communication overhead is minimized and making it advantageous for resource-constrained environments such as wireless networks. The signcryption procedure provides strong protection against data tampering and unauthorized access in the network.

Key Generation

The key generation procedure in the Kupyna Schmidt-Samoa Signcryption Model generates a pair of keys such as a private key and a public key. The private key is kept secret by the sender and it is applied for signing the data whereas the public key is distributed openly and used through the receiver to confirm signatures. A separate key is generated for encryption aspect depended on the Kupyna algorithm that enables the data remains confidential during transmission. The keys created are computationally complex to derive without access respective private key. This ensures the security of the whole signcryption process.

Consider the two various huge prime numbers 'h' and 'j' the public key of the patient is produced as given below.

$$\mu_{pub} = h^2 * j \tag{7}$$

Where μ_{pub} refers a public key. Depended on the public key, the private key is created as given below.

$$\varphi_{pri} = \frac{1}{\mu_{pub}} * mod\ z \tag{8}$$

Where $z = w\ (h-1, j-1)$ (9)

Where 'φ_{pri}' denotes a private key, μ_{pub} denotes a public key, w denotes a least common multiple factors. With this, keys are generated, and then sender carry outs signcryption process for secure transmission.

Signcryption

In the signcryption process, the sender first encrypts the data using the Schmidt-Samoa Signcryption algorithm. In signcryption step, both digital signature as well as encryption is executed at the same time. After the data is encrypted, the sender signs the encrypted data using their private key and thereby guaranteeing the integrity to the data. From this, the computation time is decreased.

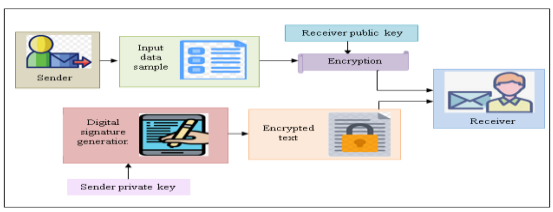

Figure 4 Process of Signcryption

Figure 4 demonstrates the block diagram of the Signcryption process involved in the Schmidt-Samoa Signcryption algorithm. The sender encrypts the data using receiver's public key. Consider the number of normal data samples $\{DS_1, DS_2, DS_3, \ldots., DS_m\}$. Then the data encryption is performed as given below.

$$Enc(q(DS)) = DS^{\mu_{pub\,(r)}} \; mod \; \mu_{pub} \tag{10}$$

Where '$Enc(q(DS))$'indicates ciphertext or encrypted data acquired depended on the receiver public key '$\mu_{pub\,(r)}$' and input data samples 'DS'. After that, the digital signature is created with the help of sender's private key. Assume the input data sample is modified into message bit $\gamma_i \in [0, 1]$. The generation digital signature is provided as follows.

$$\sigma_s = K\langle \varphi_{pri(s)} | \gamma_i \rangle \tag{11}$$

Where 'σ_s' is referred as signature and it is generated through the sender's private key '$\varphi_{pri(s)}$', hash 'K' and message bit 'γ_i'. Then, the ciphertext of data sample with the generated signature is sent to the receiver.

Unsigncryption

The proposed cryptography technique carry outs unsigncryption procedure that comprises two main steps such as signature verification and decryption at the receiver node for ensuring the security of data transmission in wireless network. The receiver needs to access the cipher text from the source node, signature verification is initially carried out and decrypt the original data sample.

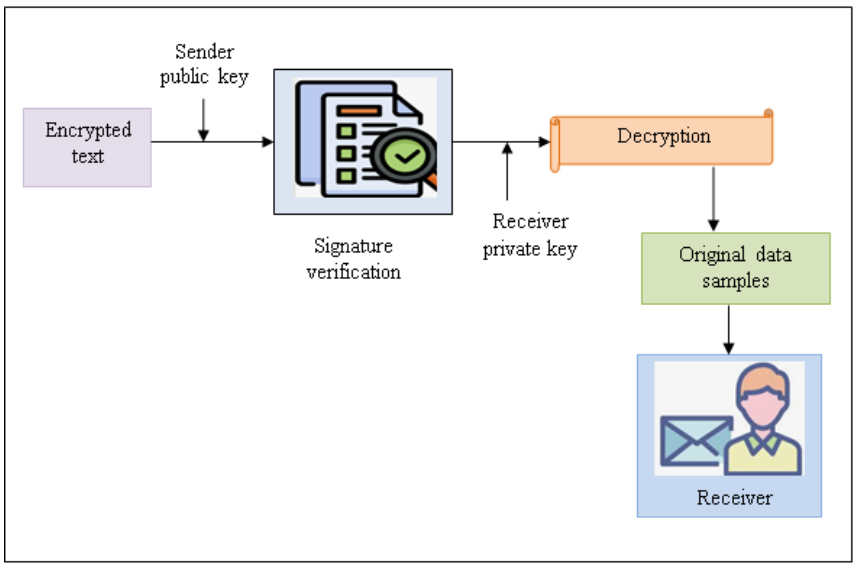

Figure 5 Process of Unsigncryption

As given in the above figure, the unsigncryption process is employed to find out the input data samples at the receiver node. Initially, the signature verification process is carried out and the signature of the received data is created using same hash function at the time of signcryption.

$$\sigma_r = K\,\langle \mu_{pub(s)} | V_i \rangle \tag{12}$$

Where 'σ_r' indicates a signature created at the receiver with senders public key '$\mu_{pub(s)}$'. Later, the generated signature is verified through the Cramer's correlation. The correlation is applied to compute the association between the two variables (i.e. signatures). Thus, the correlation between the two signatures is confirmed as follows.

$$Cra_{corr} = \left(\frac{\sum\sum|\sigma_s - \sigma_r|^2}{(m-1)+(f-1)}\right) \quad (13)$$

Where 'Cra_{corr}' refers a Cramer's Correlation coefficient, 'σ_s' refers signature generated at the sender, 'σ_r' refers a signature generated at the receiver. The output of correlation values varied from 0 to +1. Here, '0' refers no correlation between two signatures and '1' refers a high correlation between two signatures and the signature is verified. If the signature is verified, decryption is performed. Otherwise, the decryption is denied. The decryption carried out with the receiver's private key $(\varphi_{pri(r)})$ is given below.

$$DS = Enc\big(q(DS)\big)^{\varphi_{pri(r)}} mod\ uu' \quad (14)$$

Where 'DS' point outs an original data, $Enc\big(q(DS)\big)$ indicates a ciphertext, '$\varphi_{pri(r)}$' point outs a receiver's private key, $u,$ and u' point outs large prime numbers. From this, the secure communication is achieved between sender and receiver. If the receiver's private key is wrong, an additional secondary secret key is produced. This secondary key is united to a set of security questions that improves the data confidentiality. This helps to improve the overall security data transmission in wireless network. The algorithmic process of Kupyna Schmidt-Samoa Signcryption model is described as follows.

Algorithm 2: Cramer's correlated Kupyna Schmidt-Samoa Signcryption Model

Input: Number of normal data samples $DS_1, DS_2, DS_3, \ldots, DS_m$

Output: Secure data transmission

Begin

1. Gather data samples $DS_1, DS_2, DS_3, \ldots, DS_m$ // **Key generation**
2. **For** each sender node
3. Generate pair of keys
4. **End for**
5. **For** each data sample DS_i //**Signcryption**
6. Perform data encryption using receiver public key
7. Get ciphertext $Enc(q(DS)) = DS^{\mu_{pub\,(r)}}\ mod\ \mu_{pub}$
8. Generate digital signature with sender private key $\sigma_s = K\langle\varphi_{pri(s)}|\gamma_i\rangle$
9. Send ciphertext '$Enc(q(DS))$'and data samples 'σ_s' to receiver
10. **End for**
11. Receiver generates the digital signature$\sigma_r = K\langle\mu_{pub(s)}|V_i\rangle$ //**Unsigncryption**

12. Compute Cramer's correlation 'Cra_{corr}'
13. **If** ($Cra_{corr} = 1$) then
14. Signature is valid or matched
15. Decrypt the data samples
16. Get original data $DS = Enc\big(q(DS)\big)^{\varphi_{pri(r)}} mod\ uu'$
17. **Else**
18. Signature is not valid or matched
19. Decryption is not ignored
20. **End if**
21. Obtain secure data transmission

End

Algorithm 2 given above illustrates the process of Kupyna Schmidt-Samoa Signcryption model based secure data transmission in the wireless networks. The signcryption includes the three different processes such as, key generation, signcryption, and unsigncryption. Initially, generates pair of keys for each sender node. After that, sender node encrypts input data samples along with signature are generated in hash value using Cramer's correlated Kupyna Schmidt-Samoa Signcryption. Then, the data is encrypted and sent to the receiver where the unsigncryption process is carried out to ensure security. On the receiver end, signature verification is carried out using Cramer's correlation. If the signature is verified, then receiver node decrypts the data samples using receiver private key. Finally, the original data is obtained. With this, the secure data transmission is achieved in wireless network using proposed PDRDRN-KSSS technique.

4. Experimental Settings

Experimental evaluations of the proposed PDRDRN-KSSS technique is implemented using python language. The performance of cyber attack detection is analyzed by using UNSW-NB15 Dataset. The dataset is collected from https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15. The description about of dataset is given in section 3.1. In UNSW-NB15 dataset, every row is classified as normal or different kinds attack. To ensure the fair comparison, 100000 data samples is used in the result analysis. The performance of proposed PDRDRN-KSSS method is compared with conventional methods such as BSDN-HMTD and FBMP-IDS. Both the proposed and existing methods are examined in terms of different performance metrics as given below.

5. Results and Discussion

In this section, the performance of proposed PDRDRN-KSSS method technique is analyzed and compared with conventional BSDN-HMTD and FBMP-IDS in terms of different metrics such as attack detection accuracy, precision, recall, attack detection time, data confidentiality rate and data integrity rate.

5.1 Inferences

Cyber attack detection is critical in wireless network where it needs to identify the abnormal network behavior and possible intrusions. The utilization of PDRDRN-KSSS technique for offers a sophisticated, multi-layered approach for cyber security. Probabilistic Deming Regressive Similarity Indexed Deep Recursive Neural Network enhances the detection of complex, evolving threats by leveraging DL model with higher accuracy.

The attack detection model coupled with the cryptography model (Cramer's correlated Kupyna Schmidt-Samoa Signcryption) ensures robust, efficient signcryption for data in transmission. This combination gives a dynamic, adaptive defense against both known and new cyber threats.

With this, proposed PDRDRN-KSSS method offers advanced protection and real-time threat response, and efficient management of secure data transmission between sender and receiver in the wireless network is achieved. Additionally, Signcryption and Unsigncyption process during the data transmission enhances the data confidentiality and integrity in wireless networks.

5.2 Performance of Attack detection accuracy

It is defined as the proportion of number of data samples rightly categorized as attacks or normal to the total data samples. Attack detection accuracy is computed as given below.

$$ADA = \left(\frac{T_p + T_n}{T_p + F_p + T_n + F_n}\right) * 100 \quad (15)$$

Where '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 (%)		
	PDRDRN-KSSS	BSDN-HMTD [1]	FBMP-IDS [2]
10000	96.8	91.58	90.45
20000	96.98	91.62	90.12
30000	98.63	91.89	90.58
40000	97.52	92.36	90.12
50000	97.12	92.69	90.05
60000	97.63	91.25	89.25
70000	97.25	92.58	90.25
80000	96.64	92.64	89.14
90000	97.05	91.75	90.36
100000	97.12	92.63	90.68

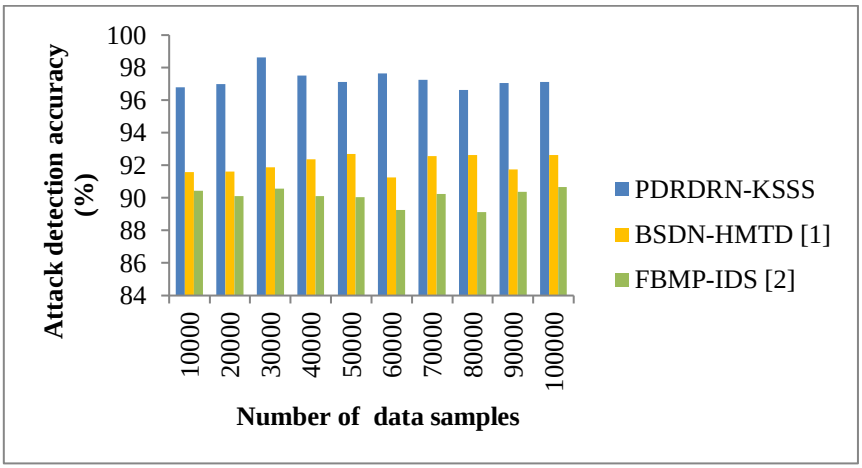

Figure 6 Results of attack detection accuracy

Figure 6 depicts the experimental results of attack detection accuracy with respect to the different number of data samples. During the simulation conduction, the performance of attack detection accuracy for proposed PDRDRN-KSSS technique is compared with the existing methods. For the experiments setup, the number of sample data is considered as a range from 10000 to 100000. Through the experiments, the attack detection accuracy is successfully increased with the help of all the three methods. As compared to existing methods, attack detection accuracy using proposed PDRDRN-KSSS technique is significantly enhanced. With the input of 10000 data samples, attack detection accuracy of PDRDRN-KSSS technique is obtained as 96.8%, whereas BSDN-HMTD [1] and FBMP-IDS [2] obtains 91.58%, and 90.45% of accuracy respectively. Similarly, the accuracy result for remaining runs is computed. The average attack detection accuracy of proposed PDRDRN-KSSS technique is obtained as 6% and 8% compared to BSDN-HMTD [1] and FBMP-IDS [2] respectively. This higher accuracy is achieved through the utilization of probabilistic Deming regressive similarity indexed deep recursive network to accurately classify the data samples into normal and attack samples.

5.3 Performance of Precision

Precision is determined as the proportion of true positives to the entire number of detection. It is calculated as follows.

$$PC = \left(\frac{T_p}{T_p + F_p}\right) \quad (16)$$

Where 'PC' indicates a precision, 'T_p' point outs a true positive, 'F_p' point outs a false positive.

Table 3 Comparison of Precision

Number of data samples	Precision		
	PDRDRN-KSSS	BSDN-HMTD [1]	FBMP-IDS [2]
10000	**0.971**	**0.937**	**0.929**
20000	**0.979**	0.934	0.923
30000	**0.966**	0.926	0.913

40000	**0.972**	0.936	0.918
50000	**0.976**	0.945	0.925
60000	**0.979**	0.936	0.923
70000	**0.981**	0.942	0.926
80000	**0.972**	0.931	0.923
90000	**0.985**	0.935	0.921
100000	**0.982**	0.938	0.925

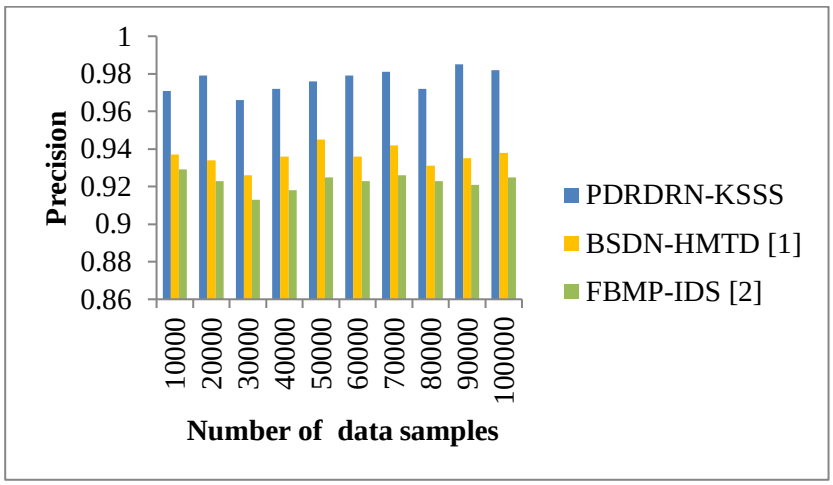

Figure 7 Results of Precision

Figure 7 illustrates the comparison of precision for data samples using proposed and existing methods. As shown in above figure, X-axis and Y-axis show the number of data samples and precision results for three methods. The blue, yellow, and green color bar represents the performance of precision using proposed PDRDRN-KSSS technique, BSDN-HMTD [1] and FBMP-IDS [2] respectively. The graphical results indicate that the performance of precision using PDRDRN-KSSS is found to be increased than the other methods. In the first run, the precision of PDRDRN-KSSS is measured as 0.971, 0.937, and 0.929 PDRDRN-KSSS technique, BSDN-HMTD [1] and FBMP-IDS [2]. In all the runs, the performance of precision is better in PDRDRN-KSSS. This significant improvement is attained using Deming Regression analysis in the classification process where it chooses the more pertinent features for attack detection. This leads to enhance the precision in PDRDRN-KSSS by 4% and 6% compared to existing BSDN-HMTD [1] and FBMP-IDS [2] respectively.

5.4 Performance of Recall

It is applied to examine the performance of a classification model. Recall computes the ratio of true positive predictions to the actual true positives and false negatives.

$$RL = \left(\frac{T_p}{T_p + F_n}\right) \quad (17)$$

Where 'RL' indicates a recall, 'T_p' refers a true positive, 'F_n' refers a false negative.

Table 4 Comparison of Recall

Number of data samples	Recall		
	PDRDRN-KSSS	BSDN-HMTD [1]	FBMP-IDS [2]
10000	0.982	0.944	0.936
20000	0.972	0.943	0.925
30000	0.982	0.942	0.927
40000	0.971	0.936	0.912
50000	0.965	0.935	0.919
60000	0.976	0.945	0.925
70000	0.975	0.935	0.912
80000	0.982	0.942	0.923
90000	0.986	0.953	0.935
100000	0.981	0.942	0.93

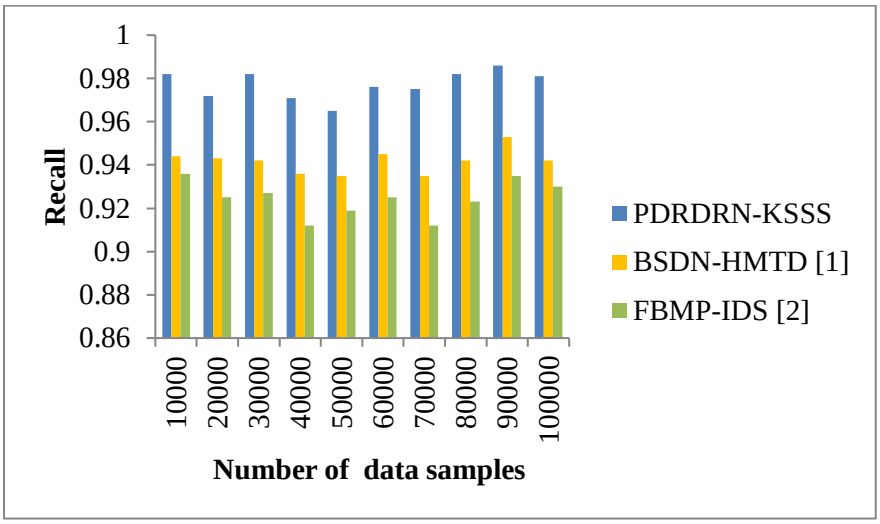

Figure 8 Results of Recall

Figure 8 depicts the performance analysis of recall for data samples using proposed PDRDRN-KSSS technique, BSDN-HMTD [1] and FBMP-IDS [2]. Horizontal axis indicates number of data samples varied from 10000 to 100000 whereas vertical axis denotes performance of recall for three methods. As depicted in above figure, the results indicate that the recall rate achieved with the PDRDRN-KSSS is relatively higher compared to existing methods [1] and [2]. The input of 10000 data samples of proposed PDRDRN-KSSS, BSDN-HMTD [1] and FBMP-IDS [2] is found to be 0.982, 0.944, and 0.936 respectively. Thus, the average comparison of recall using PDRDRN-KSSS technique is enhanced by 4% and 6% than the [1] and [2] respectively. This improvement is achieved by applying using Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network. The designed network selects the pertinent features and classifies them correctly for attack detection.

5.5 Performance of Attack detection time

It is determined as the amount of time consumed through the algorithm for attack detection. Attack detection time is detected as follows.

$$ADT = \sum_{i=1}^{n} DS_i * TM\ [CDS] \quad (18)$$

Where 'ADT' point outs the attack detection time, '$TM\ [CDS]$' point outs a time to categorize a single data samples 'DS'. The overall time is calculated in terms of milliseconds (ms).

Table 5 Comparison of Attack detection time

Number of data samples	Attack detection time (ms)		
	PDRDRN-KSSS	BSDN-HMTD [1]	FBMP-IDS [2]
10000	33	46	55
20000	41	53.2	62
30000	52.5	64.5	70
40000	60	73.6	83.6
50000	72	86.2	91.2
60000	80	91.2	99.5
70000	92	105.2	116.2
80000	99.3	115.3	120.5
90000	114	123	128.5
100000	124.3	134	143.2

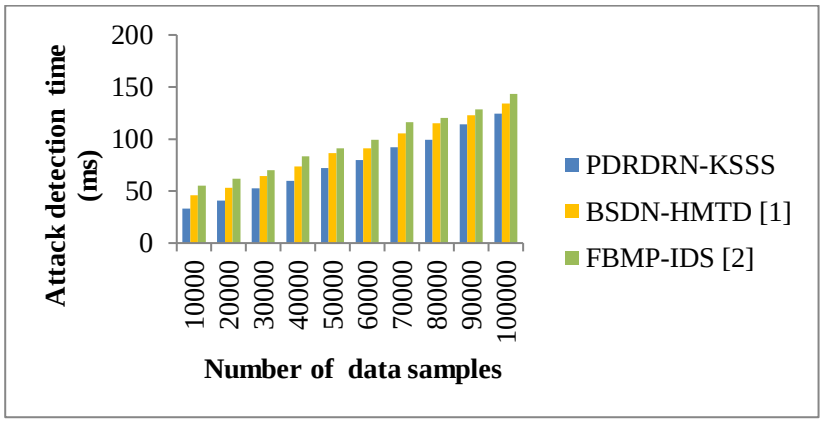

Figure 9 Results of Attack detection time

Figure 9 presents a graphical representation of the attack detection time using three methods namely PDRDRN-KSSS technique with existing methods. The graph demonstrates that attack detection time for every three methods increases as number of data samples used in the experiments increases. This is because a larger number of data samples take more time to detect the attack in the network. In experiments conducted with 10000 data samples, the time consumed for attack detection is 33ms, 46ms and 55ms using PDRDRN-KSSS technique, BSDN-HMTD [1] and FBMP-IDS [2].

Overall, outcomes denote the PDRDRN-KSSS technique significantly reduces time consumption of attack detection by 16% and 23% compared to methods [1] and [2] respectively. The lesser time consumption is attained by using Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network. The network initially chooses the features that are more contributed for attack detection. The identification attack detection via these features considerably minimizes the time consumption.

5.6 Performance of Data confidentiality rate

It is calculated as the proportion of the number of data samples are secured from the illegal access in the data transmission.

$$DCR = \sum_{i=1}^{n} \left(\frac{Secured\ DS_i}{DS_i} \right) * 100 \qquad (19)$$

Where 'DCR' refers a data confidentiality rate, '$Secured\ DS_i$' refers a number of data samples secured.

Table 6 Comparison of Data confidentiality rate

Number of data samples	Data confidentiality rate (%)		
	PDRDRN-KSSS	BSDN-HMTD [1]	FBMP-IDS [2]
10000	99.45	95.25	93.25
20000	98.25	95.21	92.36
30000	98.56	94.25	91.45
40000	99.00	94.36	92.63
50000	99.2	95.32	92.45
60000	98.25	94.23	92.33
70000	98.96	95.15	92.54
80000	98.25	94.36	92.05
90000	98.64	95.36	93.41
100000	98.46	94.25	92.36

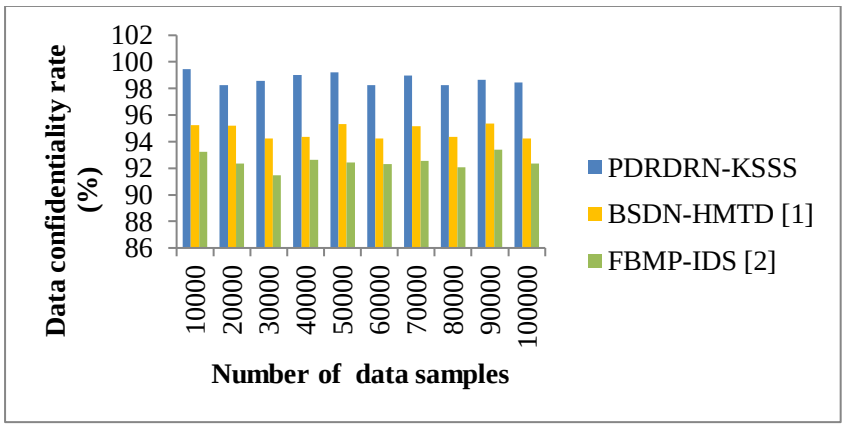

Figure 10 Results of data confidentiality rate

Figure 10 depicts the performance analysis of data confidentiality rate based on the data samples collected from given dataset. The results of data confidentiality rate using proposed PDRDRN-KSSS technique is computed and compared with existing BSDN-HMTD [1] and FBMP-IDS [2]. In the above figure, 'x' axis indicates number of data samples and 'y' axis denotes data confidentiality rate for three methods. Overall performance outcome indicates that the PDRDRN-KSSS technique enhances data confidentiality rate compared to other techniques. With this, the data confidentiality rate of PDRDRN-KSSS technique is improved by 4% and 7% as compared to existing BSDN-HMTD [1] and FBMP-IDS [2] respectively. This improvement is achieved by applying the Kupyna Schmidt-Samoa Signcryption model to securely transmit the data in the network. Here, the digital signature is used to sign the encrypted data. At the receiver side, signature verification is performed to obtain the original data. This increases the data confidentiality rate in PDRDRN-KSSS technique.

5.7 Performance of Data integrity rate

It is referred to the number of data samples that are not altered by unauthorized users to the total number of data samples. The data integrity rate is measured as given below,

$$DIR = \left[\frac{NDS_{na}}{DS_i}\right] * 100 \quad (20)$$

Where DIR denotes a data integrity rate that computed based on the 'NDS_{na}' data samples not altered to the total data samples 'DS_i'.

Table 7 Comparison of Data integrity rate

Number of data samples	Data integrity rate (%)		
	PDRDRN-KSSS	BSDN-HMTD [1]	FBMP-IDS [2]
10000	98.25	93.25	91.25
20000	98.36	93.14	91.63
30000	98.62	93.65	91.82
40000	98.12	93.54	91.45
50000	98.25	93	91.22
60000	98.25	93.11	90.63
70000	97	93.54	90.82
80000	98.11	93.82	91.36
90000	98.36	93.45	91.25
100000	98.41	93.14	91.42

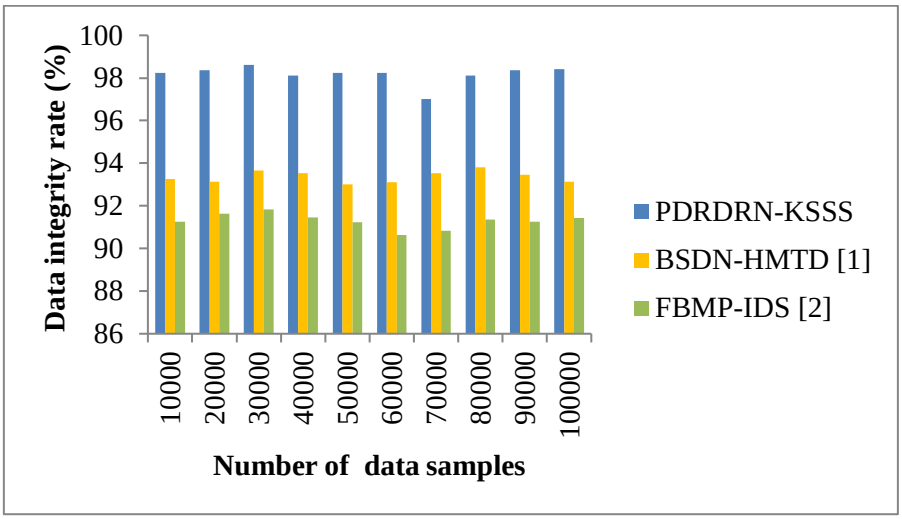

Figure 11 Results of data integrity rate

Figure 11 depict the experimental results of data integrity rate using PDRDRN-KSSS technique, existing BSDN-HMTD [1] and FBMP-IDS [2]. The data integrity rate is measured with respect to a number of data samples in the ranges from 10000 to 100000. The obtained results reveal that the precision is considerably increased by using the PDRDRN-KSSS than the other two deep learning methods. Let us consider the 10000 data samples to perform experiments. The data integrity rate of proposed PDRDRN-KSSS is achieved as 98.25%, BSDN-HMTD [1] is achieved as 93.25%, and FBMP-IDS [2] is achieved as 91.25% respectively. In the same way, the remaining results are observed for each method with different counts of input data samples. The average of ten results indicates that the PDRDRN-KSSS increases the performance of the data integrity rate by 5% and 8% when compared to existing [1] and [2] respectively. This is because of using Kupyna Schmidt-Samoa Signcryption algorithm where it performs signcryption and unsigncryption for secure data transmission.

6. Conclusion

In this paper, a new secure data transmission technique called Probabilistic Deming Regressive Deep Recursive Network based Kupyna Schmidt-Samoa Signcryption (PDRDRN-KSSS) technique is introduced. The designed technique combines attack detection and secure transmission technique. Probabilistic Deming Regressive Similarity Indexed Deep Recursive Network is designed to classify the data samples into normal and attack samples for accurate cyber attack detection. Probabilistic Deming Regression analysis is used to choose the pertinent features to reduce time consumption involved in the attack detection. With the selected features, similarity index between data samples are computed to classify the data for attack detection. To securely transmit the data samples, Cramer's correlated Kupyna Schmidt-Samoa Signcryption algorithm is applied for attaining the data integrity and confidentiality. The designed method includes the advantages of combining signing and encryption into a single process that enhances the security, efficiency and overall performance. Experimental evaluation is performed by using the UNSW-NB15 dataset. The obtained results confirm that the PDRDRN-KSSS technique increases the attack detection accuracy, precision, recall, data confidentiality, integrity with minimal time than the state-of-the-art methods.

References

[1] Parthasarathy Ramadass, Raja shree Sekar b, Saravanan Srinivasan, Sandeep Kumar Mathivanan, Basu Dev Shivahare, Saurav Mallik, Naim Ahmad, and Wade Ghribi, "BSDN-HMTD: A blockchain supported SDN framework for detecting DDoS attacks using deep learning method", Egyptian Informatics Journal, Elsevier, Volume 27, 2024, Pages 1-18

[2] Sabrina Sakraoui, Ahmed Ahmim, Makhlouf Derdour, Marwa Ahmim, Sarra Namane, and Imed Ben Dhaou, "FBMP-IDS: FL-Based Blockchain-Powered Lightweight MPC-Secured IDS for 6G Networks", IEEE Access, Volume: 12, 2024, Pages 105887 – 105905

[3] G. Ganapathy, SujathaJamuna Anand, M. Jayaprakash, S. Lakshmi, V. Banu Priya, Samuthira Pandi V, "A blockchain based federated deep learning model for secured data transmission in healthcare Iot networks", Measurement: Sensors, Elsevier, Volume 33, June 2024, Pages 1-9

[4] Rafidah Ahmad, Jagadheswaran Rajendran, Widad Ismail, "Parallel-pipelined-memory Blowfish FPGA-based radio system with improved power-throughput for secured IoT network", Ain Shams Engineering Journal, Volume 15, Issue 4, 2024, Pages 1-13

[5] Ruqaya Abdulhasan Abed, Ekhlas Kadhum Hamza, Amjad J. Humaidi, "A modified CNN-IDS model for enhancing the efficacy of intrusion detection system", Measurement: Sensors, Volume 35, 2024, Pages 1-11

[6] Farhan Ullah, Shamsher Ullah, Gautam Srivastava , Jerry Chun-Wei Lin, "IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic", Digital Communications and Networks, Volume 10, Issue 1, February 2024, Pages 190-204

[7] Lambert Kofi Gyan Danquah, Stanley Yaw Appiah, Victoria Adzovi Mantey, Iddrisu Danlard b , Emmanuel Kofi Akowuah, "Computationally Efficient Deep Federated Learning with Optimized Feature Selection for IoT Botnet Attack Detection", Intelligent Systems with Applications, Volume 25, March 2025, Pages 1-9

[8] Mansi H. Bhavsar, Yohannes B. Bekele, Kaushik Roy, John C. Kelly, And Daniel Limbrick, "FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT", IEEE Access, Volume 12, 2024, Pages 52215 – 52226

[9] K. Sedhuramalingam, N. Saravanakumar, "A novel optimal deep learning approach for designing intrusion detection system in wireless sensor networks", Egyptian Informatics Journal, Volume 27, September 2024, Pages 1-8

[10] Osama A. Khashan, "Blockchain-machine learning fusion for enhanced malicious node detection in wireless sensor networks", Knowledge-Based Systems, Volume 304, 25 November 2024, Pages 1-16

[11] Rizwan Hamid Randhawa, Nauman Aslam, Mohammad Alauthman, Muhammad Khalid, Husnain Rafiq,"Deep reinforcement learning based Evasion Generative Adversarial Network for botnet detection", Future Generation Computer Systems, Volume 150, January 2024, Pages 294-302

[12] Monika Vishwakarma, Nishtha Kesswani, “DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT”, Decision Analytics Journal, Volume 5, December 2022, Pages 1-9

[13] Jalal Bhayo, Syed Attique Shah, Sufian Hameed, Awais Ahmed, Jamal Nasir, Dirk Draheim, “Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks”, Engineering Applications of Artificial Intelligence, Volume 123, Part C, August 2023, Pages 1-17

[14] Heba Kadry, Ahmed Farouk, Elnomery A. Zanaty, Omar Reyad, “Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security”, Alexandria Engineering Journal, Volume 71, 15 May 2023, Pages 491-500

[15] Yazan A. Alsariera, Waleed Fayez Awwad, Abeer D. Algarni, Hela Elmannai, Margarita Gamarra, José Escorcia-Gutierrez, “Enhanced Dwarf Mongoose optimization algorithm with deep learning-based attack detection for drones”, Alexandria Engineering Journal, Volume 93, April 2024, Pages 59-66

[16] P. Sathishkumar, A. Gnanabaskaran, M. Saradha, R. Gopinath, “Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network”, Ain Shams Engineering Journal, Volume 15, Issue 12, December 2024, Pages 1-16

[17] Suriyan Kannadhasan, Ramalingam Nagarajan, “Intrusion detection in machine learning based E-shaped structure with algorithms, strategies and applications in wireless sensor networks”, Heliyon, Volume 10, Issue 9, 15 May 2024, Pages 1-23

[18] P. Ramadevi, S. Ayyasamy, Yalla Suryaprakash, Chunduru Anilkumar, S. Vijayakumar, R. Sudha, “Security for wireless sensor networks using cryptography”, Measurement: Sensors, Volume 29, October 2023, Pages 1-6

[19] Mehdi Selem, Farah Jemili, Ouajdi Korbaa, “Deep Learning for Intrusion Detection in IoT Networks”, Peer-to-Peer Networking and Applications, 2024, Pages 1-33

[20] Christian Callegari, Stefano Giordano, Michele Pagano, “A Real Time Deep Learning Based Approach for Detecting Network Attacks”, Big Data Research, 2024, Pages 1-12

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

[22] Hanjabam Saratchandra Sharma, Arindam Sarkar, Moirangthem Marjit Singh, “An efficient deep learning based solution for network intrusion detection in wireless sensor network”, International Journal of System Assurance Engineering and Management, Volume 14, pages 2023, Pages 2423–2446

[23] Shaymaa Mahmood Naser, Yossra Hussain Ali, Dhiya Al-Jumeily OBE, “Hybrid Cyber-Security Model for Attacks Detection Based on Deep and Machine Learning”, International Journal of Online and Biomedical Engineering (iJOE), 2022, Pages 1-30

[24] Bhukya Madhu, M. Venu Gopala Chari, Ramdas Vankdothu, Arun Kumar Silivery, Veerender Aerranagula, “Intrusion detection models for IOT networks via deep learning approaches”, Measurement: Sensors, Volume 25, 2023, Pages 1-14

[25] Olivia Jullian, Beatriz Otero, Eva Rodriguez, Norma Gutierrez, Héctor Antona & Ramon Canal, Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework, Journal of Network and Systems Management, Volume 31, 2023, Pages 1-24

[26] M. Nivaashini, E. Suganya, S. Sountharrajan, M. Prabu3 and Durga Prasad Bavirisetti, “FEDDBN-IDS: federated deep belief network based wireless network intrusion detection system”, EURASIP Journal on Information Security, volume 2024, Pages 1-20

[27] Muhammad Sajid, Kaleem Razzaq Malik1, Ahmad Almogren, Tauqeer Safdar Malik, Ali Haider Khan, Jawad Tanveer and Ateeq Ur Rehman, “Enhancing intrusion detection: a hybrid machine and deep learning approach”, Journal of Cloud Computing: Advances, Systems and Applications, 2024, Pages 1-24

[28] Salim Salmi and Lahcen Oughdir, “Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network”, Journal of Big Data, 2023, Pages 1-25

[29] Mohamed H. Behiry and Mohammed Aly, “Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods”, Journal of Big Data, 2024, Pages 1-39

[30] Syed Shahul Hameed M, V. Akshay, Vishwanadham Mandala, Chunduru Anilkumar, P. VishnuRaja, R. Aarthi, “Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things”, Measurement: Sensors, Volume 30, December 2023, Pages 1-8