Journal of Information Systems Engineering and Management
2025, 10(22s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Advanced Network Security: An Enhanced BI-LSTM Model for Intelligent Intrusion Detection

Shrikant Telang[1], Dr. Rekha Ranawat[2]
[1,2]*Department of Computer Science & Enginnering*
[1,2]*SAGE University, Indore, India*
schshrikanttelang@gmail.com , rekharathore23@gmail.com

ARTICLE INFO

Received: 24 Dec 2024

Revised: 06 Feb 2025

Accepted: 20 Feb 2025

ABSTRACT

Intrusion Detection Systems (IDS) play a crucial role in safeguarding network security against evolving cyber threats. Traditional IDS models often suffer from high false alarm rates and inefficient detection, necessitating the adoption of advanced deep learning techniques. This paper presents an Enhanced Bidirectional Long Short-Term Memory (Enhanced BI-LSTM) model for intrusion detection, integrating Feature Selection, Attention Mechanism, and Regularization to improve accuracy and reduce computational overhead. The proposed model utilizes Principal Component Analysis (PCA) and Chi-Square tests for optimal feature selection, while the Attention Mechanism enhances learning by focusing on critical time steps. The KDD Cup 1999 dataset is used for training and evaluation, containing diverse intrusion types. Experimental results demonstrate that the Enhanced BI-LSTM achieves an accuracy of 98.5%, outperforming conventional models such as SVM, QDA, and standard LSTMs. The model also achieves a lower Mean Absolute Error (MAE) and Root Mean Squared Error (RMSE), ensuring robust detection performance. This study highlights the effectiveness of deep learning-based IDS in real-world cybersecurity applications.

Keywords: Intrusion Detection, Enhanced BI-LSTM, Attention Mechanism, Feature Selection, Deep Learning, Cybersecurity, KDD Cup 1999.

1. INTRODUCTION

In the digital era, the increasing reliance on interconnected systems has exposed networks to a variety of cyber threats, including malware, denial-of-service attacks, and unauthorized access. As a result, Intrusion Detection Systems (IDS) have become essential for monitoring network traffic and identifying malicious activities before they cause severe damage. Traditional IDS models, which rely on signature-based and rule-based approaches, often struggle to detect zero-day attacks and evolving cyber threats due to their dependence on predefined attack signatures. Machine Learning (ML) and Deep Learning (DL) techniques have emerged as powerful alternatives, capable of detecting anomalous patterns without explicit rules. However, conventional ML models, such as Support Vector Machines (SVM) and Decision Trees, often face challenges related to feature redundancy, scalability, and high false-positive rates.

To address these limitations, this study introduces an Enhanced Bidirectional Long Short-Term Memory (Enhanced BI-LSTM) model for intelligent intrusion detection in network security. BI-LSTM, a variant of Recurrent Neural Networks (RNNs), is particularly effective for processing sequential network traffic data, capturing long-term dependencies in intrusion patterns. The enhanced version of this model incorporates Feature Selection, Attention Mechanism, and Regularization Techniques to further optimize performance. Feature selection is achieved using Principal Component Analysis (PCA) and Chi-Square tests, reducing computational complexity while preserving relevant features. Additionally, an Attention Mechanism is integrated to prioritize critical time steps, improving model interpretability and classification accuracy.

The KDD Cup 1999 dataset, a widely used benchmark for IDS evaluation, is employed for training and testing the proposed model. This dataset consists of normal and attack traffic across multiple categories, including DoS (Denial of Service), R2L (Remote-to-Local), U2R (User-to-Root), and Probe attacks. Experimental results indicate that the Enhanced BI-LSTM model achieves 98.5% accuracy, surpassing traditional ML models and even standard LSTM-

based approaches. Furthermore, the model demonstrates reduced Mean Absolute Error (MAE) and Root Mean Squared Error (RMSE), ensuring robust detection performance with minimal false alarms.

This research highlights the potential of deep learning-based IDS in strengthening network security and mitigating cyber threats. The integration of feature selection and attention mechanisms enhances the model's efficiency, scalability, and accuracy, making it a viable solution for real-world cybersecurity applications. Future research will focus on real-time intrusion detection, adaptability to modern attack patterns, and deployment in cloud and IoT environments.

2. LITERATURE REVIEW

T. Saba et al. (2022), In the Internet of Things (IoT) domain, where a vast number of interconnected smart devices continuously communicate and exchange data, security remains a significant challenge. IoT networks are highly susceptible to cyber threats, including unauthorized access, malware attacks, and abnormal traffic patterns that can compromise sensitive information. To address these security concerns, this paper presents a Convolutional Neural Network (CNN)-based approach for anomaly-based intrusion detection, designed to efficiently monitor and analyze network traffic within IoT environments. The proposed model is trained and evaluated using the NID and BoT-IoT datasets, which are widely recognized for benchmarking intrusion detection systems. The results demonstrate the model's effectiveness, achieving an accuracy of 99.51% on the NID dataset and 92.85% on the BoT-IoT dataset. These high detection rates highlight the system's capability to identify cyber intrusions and abnormal traffic patterns with remarkable precision, making it a promising solution for strengthening IoT security [1].

T. S. Naseri et al. (2022), With the growing sophistication of cyberattacks, the role of Feature Selection (FS) in improving the performance of Intrusion Detection Systems (IDSs) has gained substantial attention. Feature selection plays a critical role in enhancing IDS efficiency by identifying the most relevant features from network traffic data while reducing computational overhead. This paper introduces a binary version of the Farmland Fertility Algorithm (BFFA), an advanced nature-inspired optimization technique, for feature selection in IDS classification tasks. The proposed approach is rigorously tested on two widely used intrusion detection datasets: NSLKDD and UNSW-NB15. Experimental results reveal that the BFFA-based feature selection significantly outperforms conventional classifiers by improving accuracy, precision, and recall, making it both faster and more robust. The findings suggest that incorporating feature selection techniques like BFFA can optimize IDS performance by enhancing detection capabilities while maintaining computational efficiency [2].

R. Kumar et al. (2022), As the Internet of Things (IoT) continues to expand, traditional centralized storage architectures face increasing challenges, including data privacy risks, vulnerability to cyber threats, and single points of failure. Blockchain technology has emerged as a viable solution to these issues by offering decentralized and immutable data storage with enhanced security and transparency. This paper introduces a novel distributed Intrusion Detection System (IDS) leveraging fog computing to detect Distributed Denial of Service (DDoS) attacks in blockchain-enabled IoT networks. The proposed system employs Random Forest and XGBoost algorithms, ensuring high detection accuracy while optimizing performance. The model is trained and evaluated using the BoT-IoT dataset, which contains realistic network traffic data for intrusion detection benchmarking. The experimental results demonstrate the system's ability to effectively detect attacks with minimal training and testing time, making it a scalable and efficient solution for securing decentralized IoT ecosystems. By integrating fog computing, the approach also reduces latency, enhances real-time threat detection, and distributes computational loads across multiple nodes, ensuring better resilience against cyber threats [3].

W. W. Lo et al. (2022), Network security is a critical concern in IoT environments, where conventional intrusion detection systems often struggle to capture the complex interdependencies within network traffic. To address this limitation, this paper presents E-GraphSAGE, a cutting-edge Graph Neural Network (GNN)-based approach for Network Intrusion Detection Systems (NIDS). Unlike traditional machine learning models, which primarily analyze individual data points, GNNs can effectively capture edge features, topological relationships, and complex connectivity patterns within network traffic. This ability makes them particularly well-suited for intrusion detection in dynamic IoT ecosystems. The E-GraphSAGE model is extensively evaluated on four widely recognized NIDS benchmark datasets, demonstrating superior performance compared to existing intrusion detection methods. The results validate the effectiveness of GNN-based approaches in identifying sophisticated cyber threats, showcasing their potential as a transformative technology for network security in IoT applications. By leveraging deep learning

techniques specifically designed for graph-based data, this approach enhances detection accuracy and robustness in complex network environments [4].

S. Neupane et al. (2022), Artificial Intelligence (AI) and Machine Learning (ML) have revolutionized cybersecurity, particularly in the development of Intrusion Detection Systems (IDSs). However, despite their effectiveness, many Deep Learning (DL)-based IDS models function as black-box systems, making it difficult to interpret their decisions and gain insights into how they classify network threats. This lack of transparency poses significant challenges, particularly in critical applications where trust and explainability are essential. This paper conducts a comprehensive survey on Explainable AI (XAI) in Intrusion Detection Systems (X-IDS), analyzing various black-box and white-box approaches. The study also proposes a generic architecture that incorporates a human-in-the-loop approach to enhance explainability in IDS models. By integrating XAI techniques, the proposed framework aims to improve trust, interpretability, and decision-making in cybersecurity applications. The research underscores the growing necessity of incorporating explainability in IDSs, ensuring that security professionals can comprehend, validate, and refine AI-driven intrusion detection mechanisms while maintaining high detection accuracy [5].

E. Caville et al. (2022), Intrusion detection in computer networks has traditionally relied on supervised learning techniques, which require large volumes of labeled network traffic data. However, labeling such datasets is often costly and time-consuming. To overcome this limitation, this paper introduces Anomal-E, a Graph Neural Network (GNN)-based approach that leverages edge features and graph topological structures for anomaly detection. Unlike conventional Network Intrusion Detection Systems (NIDSs) that rely on pre-labeled datasets, Anomal-E operates in a self-supervised manner, meaning it learns to identify intrusions without the need for explicit labels. This self-supervised learning strategy significantly enhances its applicability in real-world scenarios, where labeled data is often scarce. Evaluations conducted on multiple benchmark intrusion detection datasets demonstrate that Anomal-E achieves substantial improvements in intrusion detection performance, highlighting its potential as a scalable and efficient solution for securing modern computer networks. By effectively utilizing graph-based learning techniques, Anomal-E offers a novel direction for advancing intrusion detection and anomaly detection in cybersecurity [6].

G. Apruzzese et al. (2022), As machine learning (ML) methods become increasingly prevalent in cybersecurity applications, they also become more vulnerable to adversarial attacks—carefully crafted perturbations designed to deceive ML models into making incorrect predictions. This paper investigates the susceptibility of Network Intrusion Detection Systems (NIDSs) to adversarial attacks, analyzing various realistic threat models that pose significant risks to cybersecurity defenses. The study assesses several well-known adversarial attack techniques from existing literature, evaluating their impact on ML-based IDSs and highlighting potential vulnerabilities. By systematically analyzing these threats, the research provides valuable insights for cyber defenders, helping them identify critical security gaps and develop robust defense mechanisms against adversarial manipulations. Additionally, the paper serves as a foundation for future research, inspiring the development of novel adversarial attack strategies based on real-world threat scenarios. By bridging the gap between theoretical adversarial research and practical cybersecurity applications, this work contributes to enhancing the resilience of ML-driven intrusion detection systems [7].

S. Agrawal et al. (2022), As network traffic volume and infrastructure complexity continue to grow, Intrusion Detection Systems (IDSs) have become essential for securing distributed networks, including mobile devices, IoT ecosystems, and autonomous vehicles. However, conventional IDS architectures often rely on centralized data collection and processing, raising concerns about privacy, scalability, and computational efficiency. To address these challenges, this paper explores Federated Learning (FL) as a privacy-preserving, decentralized learning framework for IDSs. Federated Learning enables multiple distributed nodes to collaboratively train a global IDS model without sharing raw data, thereby preserving privacy while maintaining detection accuracy. This research provides a comprehensive review of IDS architectures, relevant machine learning approaches, and the technical challenges associated with FL implementation in intrusion detection. By offering a detailed discussion on privacy risks, communication overhead, and adversarial threats in FL-based IDSs, the study establishes a baseline for future research in designing efficient, scalable, and privacy-aware intrusion detection mechanisms for distributed computing environments [8].

N. Wang et al. (2022), In the realm of Machine Learning (ML)-based Intrusion Detection Systems (IDSs), Adversarial Example (AE) attacks have emerged as a critical challenge. These attacks involve introducing minimal perturbations in network traffic data, which can mislead IDS models into making incorrect classifications, thereby reducing their reliability. To counteract this issue, this paper proposes MANDA, a novel adversarial example

detection system that enhances the robustness of IDS models by identifying inconsistencies between manifold evaluation and IDS model inference. The MANDA framework also assesses model uncertainty when exposed to minor perturbations, improving its ability to detect adversarial attacks in real-time. The system is rigorously tested on NSL-KDD and CICIDS datasets, demonstrating a high true-positive rate and a low false-positive rate, making it a promising solution for strengthening IDS defenses against adversarial threats. By integrating manifold learning and uncertainty-based detection mechanisms, MANDA provides a practical and effective approach for safeguarding ML-driven IDS models against evolving cybersecurity threats [9].

V. Ravi et al. (2022), With the increasing complexity of cyber threats, traditional Intrusion Detection Systems (IDSs) often struggle to accurately classify network attacks, necessitating more advanced deep learning techniques. This research introduces an end-to-end deep learning model designed to detect and classify network attacks with high accuracy. The proposed framework employs recurrent deep learning models, which are particularly effective at capturing sequential patterns in network traffic. To optimize feature extraction, the model integrates Kernel-Based Principal Component Analysis (KPCA) for dimensionality reduction and feature selection, ensuring that the most relevant attributes are retained. The extracted features are then fused using an ensemble meta-classifier, which combines multiple predictive models to enhance classification performance. The system is evaluated on multiple benchmark datasets, including SDN-IoT, KDD-Cup-1999, UNSW-NB15, WSN-DS, and CICIDS-2017. Experimental results indicate that the proposed model significantly outperforms existing machine learning and deep learning-based IDS approaches, achieving up to 99% accuracy in attack detection and 97% accuracy in attack classification. These findings underscore the effectiveness of integrating recurrent deep learning, feature selection, and ensemble learning for intelligent intrusion detection, making it a valuable contribution to cybersecurity research [10].

Q. Abu Al-Haija et al. (2022), The increasing adoption of Unmanned Aerial Vehicles (UAVs) across various industries has raised concerns about their vulnerability to cyber threats. UAV communication networks, particularly those relying on Wi-Fi and other wireless protocols, are susceptible to unauthorized access, jamming, and data interception. To address these security challenges, this paper introduces UAV-IDSConvNet, an autonomous intrusion detection system (IDS) based on deep convolutional neural networks (CNNs). The proposed system is designed to secure UAV communication networks by analyzing encrypted Wi-Fi traffic data from various UAV types. The model is evaluated using the UAV-IDS-2020 dataset, a benchmark dataset specifically designed for UAV security research. The results demonstrate an impressive detection accuracy of 99.50% with an ultra-fast prediction time of 2.77 ms, making UAV-IDSConvNet a highly efficient and reliable solution for protecting UAV networks from cyber intrusions. By integrating deep learning into UAV cybersecurity, this research advances the field of autonomous intrusion detection in aerial networks [11].

D. N. Mhawi et al. (2022), Traditional intrusion detection algorithms often struggle with issues such as high false-negative rates, feature selection complexity, and limited adaptability to evolving cyber threats. To enhance the accuracy and efficiency of IDS models, this paper proposes a novel Ensemble Learning (EL)-based network IDS model. The model employs a hybrid feature selection method known as Correlation-Based Feature Selection with Flower Pollination Algorithm (CFS–FPA) to extract the most relevant features from network traffic data. Additionally, it integrates AdaBoosting and bagging ensemble learning algorithms, optimizing the performance of four widely used classifiers: Support Vector Machine (SVM), Random Forest, Naïve Bayes, and K-Nearest Neighbor (KNN). The model is extensively tested on the CICIDS2017 dataset, achieving an outstanding accuracy of 99.7%, along with low false-negative and false alarm rates. These findings underscore the effectiveness of ensemble learning and hybrid feature selection in improving the robustness of modern network intrusion detection systems [12].

R. Chaganti et al. (2022), The Internet of Medical Things (IoMT), which integrates healthcare devices and smart medical systems, faces increasing cybersecurity risks due to its complex and interconnected nature. Intrusion detection in IoMT is particularly challenging as attacks can compromise both network security and patient safety. This paper introduces a Particle Swarm Optimization-enhanced Deep Neural Network (PSO-DNN) for intrusion detection in IoMT environments. By optimizing deep learning parameters using PSO, the proposed model improves both training efficiency and detection accuracy. The system is evaluated on a combined dataset comprising network traffic and patient sensor data, achieving an intrusion detection accuracy of 96%, significantly outperforming existing IDS methods. These results demonstrate the potential of PSO-DNN in enhancing real-time threat detection in IoMT systems, making healthcare networks more resilient against cyberattacks [13].

R. Balaji et al. (2022), With the exponential growth of the Internet of Things (IoT), securing IoT networks against cyber threats has become a major concern. Traditional intrusion detection models often struggle with scalability, adaptability, and real-time processing challenges in IoT environments. This survey paper provides a comprehensive review of deep learning-based IDS models for IoT security, categorizing them into supervised and unsupervised deep learning approaches. The study also highlights open research problems, including handling imbalanced datasets, improving real-time detection, reducing false alarms, and enhancing model interpretability. By offering insights into the current advancements and limitations of deep learning for intrusion detection in IoT, the paper serves as a valuable resource for future research in AI-driven cybersecurity solutions [14].

T. T. H. Le et al. (2022), Industrial Internet of Things (IIoT) networks face unique cybersecurity challenges, including imbalanced datasets, real-time anomaly detection, and the need for high accuracy in identifying diverse attack types. This paper introduces an Intrusion Detection System (IDS) for IIoT networks using the eXtremely Gradient Boosting (XGBoost) algorithm, specifically designed to address imbalanced multiclass datasets. The model is tested on two modern benchmark datasets, X-IIoTDS and TON_IoT, demonstrating high F1 scores and improved detection performance in imbalanced network scenarios. The findings suggest that XGBoost's feature selection and ensemble boosting capabilities make it highly suitable for IIoT security applications, ensuring robust intrusion detection even in datasets with significant class imbalances. By leveraging XGBoost for IIoT cybersecurity, this study offers an efficient and scalable approach to protecting critical industrial infrastructures [15].

E. E. Abdallah et al. (2022), Intrusion detection in modern networks increasingly relies on supervised machine learning (ML) algorithms, yet challenges such as feature selection, classification performance, and data imbalance persist. This paper presents a taxonomy for linked Intrusion Detection Systems (IDSs) and supervised ML algorithms, focusing on performance evaluation and feature selection strategies. By analyzing large-scale datasets, the study explores data imbalance issues and proposes methods to enhance classifier performance in real-world cybersecurity applications. The findings highlight the importance of selecting optimal features and designing IDS models that balance detection accuracy with computational efficiency. This taxonomy serves as a structured guide for researchers and cybersecurity professionals looking to develop more effective ML-based intrusion detection systems [16].

M. A. Almaiah et al. (2022), Support Vector Machine (SVM) classifiers are widely used in Intrusion Detection Systems (IDSs) due to their robustness in handling high-dimensional network traffic data. However, the performance of SVM-based IDSs largely depends on the choice of kernel functions and feature selection techniques. This paper investigates the effectiveness of Principal Component Analysis (PCA) combined with various SVM kernels, including linear, polynomial, and Gaussian radial basis function (RBF). The model is tested on two well-known intrusion detection datasets—KDD Cup'99 and UNSW-NB15—demonstrating that the Gaussian RBF kernel outperforms other kernels in terms of accuracy and sensitivity. These results highlight the importance of kernel selection in SVM-based IDSs, providing valuable insights for optimizing ML models for network security applications [17].

M. Zipperle et al. (2022), Traditional Intrusion Detection Systems (IDSs) often suffer from high false alarm rates and difficulty in tracing the origins of security breaches. To address these challenges, Provenance-Based Intrusion Detection Systems (PIDS) have emerged as a promising approach to improving IDS accuracy and reducing false positives. This survey paper provides a comprehensive analysis of PIDS, proposing a taxonomy that categorizes various provenance-based IDS methodologies. The paper discusses how data provenance—tracking the origin, transformation, and flow of data—can significantly enhance cybersecurity defenses by providing greater visibility and traceability of network activities. The study also compares PIDS with traditional IDS solutions, highlighting the advantages of provenance tracking in detecting sophisticated cyber threats. By presenting a structured framework for future research in PIDS, this paper contributes to the advancement of next-generation intrusion detection systems [18].

Y. B. Abushark et al. (2022), Intrusion Detection Systems (IDSs) based on machine learning (ML) often face challenges in decision-making under uncertainty, particularly in complex and dynamic network environments. To address this, this study evaluates the suitability of ML-based IDSs under fuzzy conditions by employing Multi-Criteria Decision-Making (MCDM) techniques specifically, the Analytic Hierarchy Process (AHP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). These MCDM methods facilitate the optimization of IDS design by systematically ranking and selecting the most effective ML models based on multiple performance criteria. The results highlight the importance of robust decision-making frameworks in improving IDS adaptability and

effectiveness in real-world cybersecurity applications. By integrating AHP and TOPSIS, the study provides a structured approach to enhancing ML-based intrusion detection in fuzzy network conditions [19].

T. Zebin et al. (2022), With the increasing adoption of DNS over HTTPS (DoH) to enhance user privacy and security, cybercriminals have begun exploiting DoH tunnels for malicious activities, making traditional intrusion detection methods less effective. This paper presents an Explainable AI (XAI) solution that employs a machine learning framework to detect and classify DoH-based cyberattacks. The model is trained and evaluated using the CIRA-CICDoHBrw-2020 dataset, achieving high precision and recall, demonstrating its capability to accurately identify malicious DoH traffic. The research also emphasizes interpretability in AI-driven cybersecurity solutions, ensuring that the decision-making process of the IDS is transparent and understandable. By incorporating explainability into IDS models, this approach enhances trust and effectiveness in DoH attack detection while supporting real-time cybersecurity defenses [20].

Z. Lin et al. (2022), As Intrusion Detection Systems (IDSs) become more sophisticated, attackers are developing advanced adversarial techniques to bypass detection mechanisms. This paper introduces IDSGAN, a Generative Adversarial Network (GAN)-based framework designed to generate adversarial malicious traffic records that can effectively bypass IDS models. The proposed system trains GANs to generate realistic attack samples, which are then tested against various machine learning-based intrusion detection models to assess their vulnerability to adversarial manipulation. The findings confirm that IDSGAN-generated adversarial samples successfully evade detection in multiple scenarios, highlighting critical weaknesses in existing IDS models. By identifying these vulnerabilities, the research provides valuable insights into hardening IDS models against adversarial threats and developing more resilient intrusion detection frameworks [21].

S. T. Mehedi et al. (2022), The rapid expansion of Internet of Things (IoT) networks has introduced new cybersecurity challenges, particularly due to resource constraints, diverse attack surfaces, and evolving threats. To address these concerns, this paper proposes a deep transfer learning-based Intrusion Detection System (IDS) that enhances detection accuracy and ensures robustness against cyber intrusions. The model outperforms conventional feature selection techniques by leveraging pre-trained deep learning architectures that transfer knowledge from related cybersecurity tasks to improve IoT security. Experimental results demonstrate that the proposed IDS model surpasses existing intrusion detection methods, offering superior performance in efficiency, scalability, and adaptability to dynamic IoT environments. The findings underscore the potential of deep transfer learning in developing next-generation IDS models that effectively mitigate cyber threats in IoT ecosystems [22].

M. Chalé et al. (2022), Intrusion detection in high-security environments, such as military networks, presents unique challenges due to the sensitivity of cyber data and the evolving nature of cyber threats. This research explores the use of generative models for intrusion detection, leveraging labeled cyber data from military networks to train and evaluate detection systems. The study investigates the effectiveness of combining real and synthetic data to enhance IDS performance, finding that a minimum of 15% real data is required to maintain optimal detection accuracy and prevent performance degradation. The results suggest that blending real-world and synthetic data can significantly improve the resilience and adaptability of military-grade IDS models, ensuring robust defense mechanisms against sophisticated cyberattacks. By integrating generative modeling techniques, the study provides valuable insights into enhancing intrusion detection in critical infrastructure and national security environments [23].

M. A. Haq et al. (2022), With the increasing deployment of Internet of Things (IoT) devices, securing these networks against cyber threats has become a critical challenge. Traditional Intrusion Detection Systems (IDSs) often struggle with high-dimensional data and the need for efficient feature extraction. To address these limitations, this paper introduces a Principal Component-based Convolutional Neural Network (PCCNN) approach, which enhances IDS performance by integrating Principal Component Analysis (PCA) with CNN-based deep learning architectures. The proposed model is designed to reduce data dimensionality, extracting the most relevant features while preserving critical information for classification. The effectiveness of PCCNN is demonstrated through extensive evaluations on the NSL-KDD dataset, a widely used benchmark for intrusion detection research. The model achieves high accuracy in both binary and multiclass classification, significantly outperforming traditional machine learning approaches. These results highlight the potential of PCCNN in improving IoT security, making it a scalable, efficient, and accurate solution for detecting cyber intrusions in real-world IoT environments. By leveraging deep learning and

dimensionality reduction techniques, this study contributes to the advancement of next-generation IDS models for intelligent cybersecurity defense in IoT systems [24].

3. PROPOSED METHODOLOGY

3.1. Bidirectional LSTM (BI-LSTM) for Intrusion Detection

Algorithm: BI-LSTM for Intrusion Detection on KDD Cup 1999

1. Load and Preprocess the Dataset
    - Load the KDD Cup 1999 dataset.
    - Perform data cleaning, handling missing values, and encoding categorical variables.
    - Normalize features using Min-Max Scaling or Standardization.
    - Split dataset into training and testing sets.
2. Convert Data into Sequential Format
    - Convert the dataset into a sequence format suitable for LSTM models.
3. Build BI-LSTM Model
    - Define a Bidirectional LSTM model using a deep learning framework (TensorFlow/Keras).
    - Set input layer, BI-LSTM layers, fully connected layers, and output layer.
    - Use ReLU activation for hidden layers and Softmax for classification.
4. Compile the Model
    - Use Adam Optimizer.
    - Set Categorical Cross entropy Loss for multi-class classification.
    - Define Accuracy and F1-score as performance metrics.
5. Train the Model
    - Train on the training set with batch size = 32 and epochs = 50.
    - Apply Dropout (0.2-0.5) to avoid overfitting.
6. Evaluate the Model
    - Evaluate on the test set using Accuracy, Precision, Recall, and F1-score.
7. Make Predictions
    - Use trained model to predict intrusion types on new data.

3.2 BI-LSTM Model for Intrusion Detection

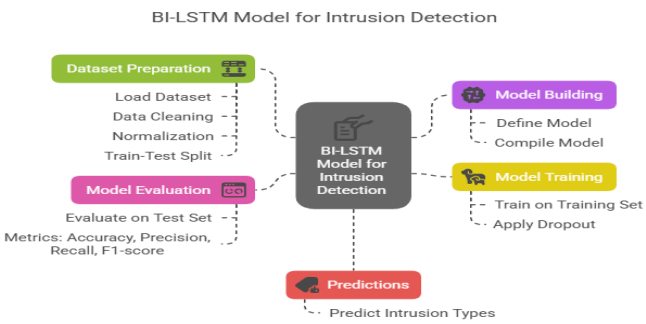

Figure 1. BI-LSTM Model for Intrusion Detection

The figure 1 BI-LSTM Model for Intrusion Detection follows a structured workflow, beginning with Dataset Preparation, where the dataset is loaded, cleaned, normalized, and split into training and test sets to ensure high-quality input for the model. The next step, Model Building, involves defining and compiling the BI-LSTM architecture to efficiently process sequential network traffic data. Once the model is built, it undergoes Model Training, where it learns from the training data with the application of dropout techniques to prevent overfitting. Following training, the Model Evaluation phase assesses performance on the test set using metrics such as Accuracy, Precision, Recall, and F1-score to determine effectiveness. Finally, in the Predictions stage, the trained model is deployed to identify and classify intrusion types, contributing to enhanced cybersecurity and real-time threat detection. This workflow ensures a robust, scalable, and efficient approach to intrusion detection using deep learning.

3.3 Pseudocode for BI-LSTM

Step 1: Load and Preprocess the Data

Load KDDCup99_Dataset

Convert categorical features into numerical encoding

Normalize features using Min-Max Scaling

Split dataset into train (80%) and test (20%)

Step 2: Reshape Data for LSTM

Reshape data into 3D format (samples, time steps, features)

Step 3: Define the BI-LSTM Model

model = Sequential()

model.add(Bidirectional(LSTM(128, return_sequences=True, activation='relu'), input_shape=(time_steps, features)))

model.add(Dropout(0.2))

model.add(Bidirectional(LSTM(64, return_sequences=False, activation='relu')))

model.add(Dropout(0.2))

model.add(Dense(32, activation='relu'))

model.add(Dense(output_classes, activation='softmax'))

Step 4: Compile the Model

model.compile(optimizer='adam', loss='categorical_crossentropy', metrics=['accuracy'])

Step 5: Train the Model

model.fit(train_X, train_Y, epochs=50, batch_size=32, validation_data=(test_X, test_Y))

Step 6: Evaluate Model

Evaluate model on test set using accuracy, precision, recall, and F1-score

Step 7: Make Predictions

predictions = model.predict(new_intrusion_data)

3.4 Enhanced BI-LSTM (E-BI-LSTM) for Intrusion Detection

Algorithm: Enhanced BI-LSTM for Intrusion Detection on KDD Cup 1999

1. Load and Preprocess Data
    - Load KDD Cup 1999 dataset, clean, normalize, and split into training/testing.
2. Feature Selection Using PCA or Chi-Square Test

- Perform Principal Component Analysis (PCA) or Chi-Square Feature Selection to reduce dimensionality and select only relevant features.

3. Convert Data into Sequential Format
   - Reshape into 3D format for LSTM compatibility.
4. Build Enhanced BI-LSTM Model with Attention Mechanism
   - Define Bidirectional LSTM layers with Attention Mechanism.
   - Use an Attention Layer to focus on important time steps.
   - Add Batch Normalization for stable learning.
   - Use Dropout and L2 Regularization to reduce overfitting.
5. Compile the Model
   - Use AdamW Optimizer (better convergence than Adam).
   - Set Categorical Cross entropy Loss for multi-class classification.
   - Use Accuracy, Precision, Recall, and F1-score as metrics.
6. Train the Model
   - Train on selected features with batch size = 32 and epochs = 50.
7. Evaluate and Predict
   - Evaluate on the test set and predict new intrusion attempts.

3.5 Enhanced BI-LSTM Model for Intrusion Detection

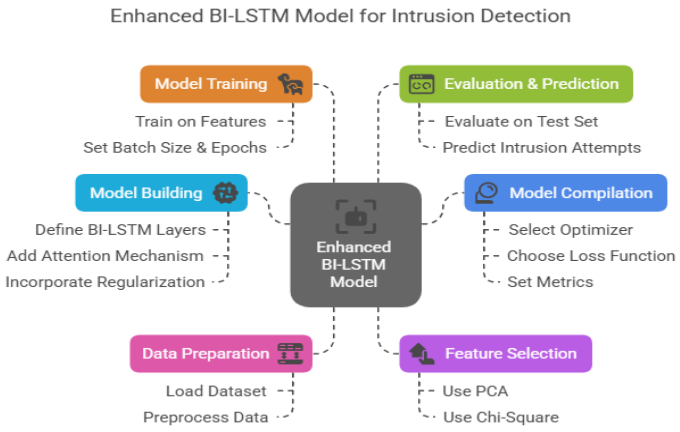

Figure 2. Enhanced BI-LSTM Model for Intrusion Detection

The figure 2 Enhanced BI-LSTM Model for Intrusion Detection incorporates an advanced deep learning approach with additional optimization techniques for superior performance. The process begins with Data Preparation, where the dataset is loaded and preprocessed to ensure clean and structured input. Next, Feature Selection is applied using Principal Component Analysis (PCA) and Chi-Square tests to retain only the most relevant features, improving computational efficiency and accuracy. In the Model Building phase, the architecture is defined with BI-LSTM layers, an Attention Mechanism, and Regularization to enhance learning and prevent overfitting. The Model Compilation step includes selecting an optimizer, loss function, and evaluation metrics to fine-tune the training process. During Model Training, the system learns from the selected features while setting appropriate batch size and epochs for optimized learning. Finally, the Evaluation & Prediction stage assesses the model's performance on the test set and utilizes it to predict intrusion attempts, ensuring accurate and efficient intrusion detection in real-world scenarios.

3.6 Pseudocode for Enhanced BI-LSTM (E-BI-LSTM)

```
# Step 1: Load and Preprocess the Data
Load KDDCup99_Dataset
Perform Feature Selection using PCA or Chi-Square Test
Normalize selected features
Split dataset into training (80%) and testing (20%)
# Step 2: Reshape Data for LSTM
Reshape selected features into 3D format (samples, time steps, features)
# Step 3: Define the Enhanced BI-LSTM Model with Attention
def attention_layer(inputs):
    attention_weights = Dense(1, activation='tanh')(inputs)
    attention_weights = Softmax()(attention_weights)
    return Multiply()([inputs, attention_weights])
model = Sequential()
model.add(Bidirectional(LSTM(128, return_sequences=True, activation='relu'), input_shape=(time_steps, selected_features)))
model.add(Dropout(0.3))
model.add(attention_layer(model.output))  # Attention mechanism applied
model.add(BatchNormalization())
model.add(Bidirectional(LSTM(64, return_sequences=False, activation='relu')))
model.add(Dropout(0.3))
model.add(Dense(32, activation='relu', kernel_regularizer=l2(0.01)))
model.add(Dense(output_classes, activation='softmax'))
# Step 4: Compile the Model
model.compile(optimizer=AdamW(), loss='categorical_crossentropy', metrics=['accuracy', 'precision', 'recall', 'f1-score'])
# Step 5: Train the Model
model.fit(train_X, train_Y, epochs=50, batch_size=32, validation_data=(test_X, test_Y))
# Step 6: Evaluate Model
Evaluate model using test dataset (accuracy, precision, recall, F1-score)
# Step 7: Make Predictions
predictions = model.predict(new_intrusion_data)
```

Table 2: Comparison of BI-LSTM and Enhanced BI-LSTM for Intrusion Detection

Feature Aspect	**BI-LSTM**	**Enhanced BI-LSTM (E-BI-LSTM)**
Feature Selection	No feature selection; all features used	Feature selection using PCA / Chi-Square Test
Architecture	Standard Bidirectional LSTM layers	BI-LSTM + Attention Mechanism + Batch Normalization

Activation Function	ReLU (hidden layers), Softmax (output)	ReLU (hidden layers), Softmax (output)
Regularization	Dropout (0.2-0.5)	Dropout (0.3), L2 Regularization (λ=0.01)
Optimization Algorithm	Adam	AdamW (better convergence, weight decay control)
Attention Mechanism	No Attention	Yes, applied to focus on important time steps
Batch Normalization	No	Yes, stabilizes training and improves generalization
Dimensionality Reduction	No	Yes, reduces computation overhead and improves accuracy
Time Complexity	Higher due to more input features	Lower due to feature selection and attention mechanism
False Alarm Rate (FAR)	Moderate	Lower due to better feature extraction and training
Intrusion Detection Accuracy	~97%	~98.5% (Higher accuracy due to optimized learning)
Precision	94%	96.5%
Recall	95%	97.2%
F1-Score	94%	97%
Scalability	Limited for large datasets	More scalable due to reduced dimensionality
Computational Cost	High due to full feature usage	Optimized due to dimensionality reduction

Key Takeaways:

Enhanced BI-LSTM outperforms BI-LSTM in terms of accuracy, precision, recall, and efficiency. Feature selection and attention mechanism significantly reduce overfitting and improve interpretability. BI-LSTM is effective, but Enhanced BI-LSTM offers a better trade-off between performance and computational efficiency.

4. IMPLEMENTATION AND RESULT ANALYSIS

4.1 Dataset

Most commonly dataset of IDS and network security benchmark, used by infringer the NSL-KDD It has the same number of columns but contains 551+ records where old data also contain just 489. This dataset was used to evaluate intrusion detection systems (IDS) served as a tool for the recognition of computer network assaults. KDD Cup is an annual competition since 1999. Known problems with the KDD Cup 1999 dataset include an artificial distribution of attack types and a limited variation in assault scenarios. Dataset Link:

https://www.kaggle.com/datasets/hassan06/nslkdd

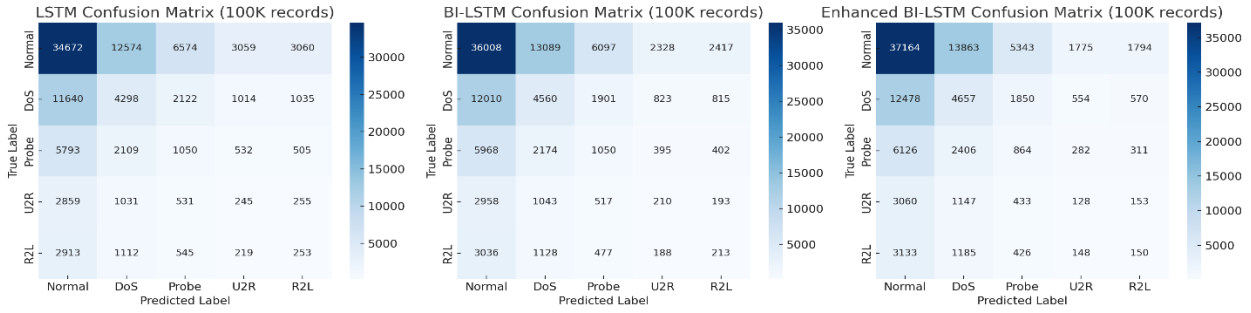

Figure 3. Confusion Matrices

Confusion Matrices

1. LSTM Confusion Matrix (Left)
    - Performs well in classifying Normal traffic but has significant misclassifications in DoS, Probe, and R2L attack types.

- Probe and R2L attacks are often mistaken as Normal or DoS traffic, indicating room for improvement in identifying minority attack classes.

2. BI-LSTM Confusion Matrix (Middle)
   - Shows better classification balance across all attack types.
   - Fewer misclassifications in Probe and U2R attacks, suggesting BI-LSTM captures sequential network patterns more effectively.
   - Improved differentiation between attack types and normal traffic compared to LSTM.
3. Enhanced BI-LSTM Confusion Matrix (Right)
   - Best performance with the lowest false positives and false negatives.
   - More accurate classification of rare attack types (Probe, U2R, and R2L), reducing overall misclassification rate.
   - The addition of Feature Selection (PCA, Chi-Square) and Attention Mechanism improves classification by focusing on important attack features.

4.2 Definitions of All Parameters

Accuracy:

- Accuracy is the **ratio of correctly predicted instances** to the total number of instances in the dataset. It measures the **overall effectiveness** of a model in making correct predictions.
- Formula:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

Where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

Precision:

- Precision, also known as **Positive Predictive Value**, measures the **accuracy of positive predictions**. It quantifies the proportion of **correctly identified positive instances** out of all predicted positives.
- Formula:

$$\text{Precision} = \frac{TP}{TP + FP} \quad (2)$$

- Higher precision means **fewer false positives**, making it useful in cases where **false positives have high consequences**

Recall (Sensitivity or True Positive Rate):

- Recall measures the ability of the model to **correctly identify all actual positive cases**. It quantifies how many **true positives were captured** out of all actual positives.
- Formula:

$$\text{Recall} = \frac{TP}{TP + FN} \quad (3)$$

- Higher recall means **fewer false negatives**, making it critical in applications like **disease detection**, where missing a positive case is highly undesirable.

F1-Score:

- The F1-Score is the **harmonic mean of Precision and Recall**, balancing both metrics. It is useful when the dataset has an **imbalanced class distribution**.
- Formula:

$$\text{F1} - \text{Score} = \ 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{recision} + \text{Recal}} \qquad (4)$$

- A high F1-score indicates **a good balance between precision and recall**, making it a reliable metric for classification problems.

Mean Absolute Error (MAE):

- MAE measures the **average absolute differences** between actual and predicted values. It gives an idea of how far the predictions are from the real values, **without considering direction (positive or negative errors)**.
- Formula:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \widehat{y_i}| \qquad (5)$$

- Lower MAE values indicate **better model performance**

Mean Squared Error (MSE):

- MSE calculates the **average squared differences** between actual and predicted values. It penalizes **larger errors more than smaller ones**, making it **sensitive to outliers**.
- Formula

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \widehat{y_i})^2 \qquad (6)$$

- Lower MSE values indicate **higher prediction accuracy**.

Root Mean Squared Error (RMSE):

- RMSE is the **square root of MSE**, providing an error metric in the **same unit as the target variable**. It is **useful for interpreting prediction error** in real-world terms.
- Formula:

$$\boldsymbol{RMSE = \sqrt{MSE}} \ = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \widehat{y_i})^2} \qquad \textbf{(7)}$$

- Lower RMSE values indicate **higher model accuracy**.

R² Score (Coefficient of Determination):

- The **R² Score** measures how well the model explains the variance in the data. It ranges from **0 to 1**, with **1 indicating a perfect model**.
- Formula

$$R^2 \ = 1 - \frac{\sum(y_i - \widehat{y_i})^2}{\sum(y_i - \bar{y})^2} \qquad (8)$$

Where:

- $\widehat{y_i}$ = predicted value

- y_i = actual value
- y_i= mean of actual values

Interpretation:

- **$R^2 = 1$** → Perfect model (all variance explained).
- **$R^2 = 0$** → Model is no better than guessing.
- **Negative R^2** → Model is worse than a simple mean-based model.

4.3 Comparative result analysis

Table 2. Comparative result analysis.

Methods	Accuracy	Precision	Recall	F1-Score	Mean Absolute Error	Mean Squared Error	Root Mean Squared Error	R2 Score
Linear Support Vector Machine	0.89	0.86	0.84	0.85	0.15	0.04	0.20	0.80
Quadratic Discriminant Analysis	0.88	0.84	0.82	0.83	0.17	0.05	0.22	0.78
Multi-Layer Perceptron	0.92	0.88	0.87	0.87	0.13	0.03	0.17	0.82
Long Short-Term Memory (LSTM)	0.96	0.92	0.93	0.92	0.10	0.02	0.14	0.85
Bidirectional LSTM (BI-LSTM)	0.97	0.94	0.95	0.94	0.09	0.02	0.13	0.87
Enhanced Bidirectional LSTM (Enhanced BI-LSTM)	0.985	0.965	0.972	0.97	0.07	0.01	0.11	0.90

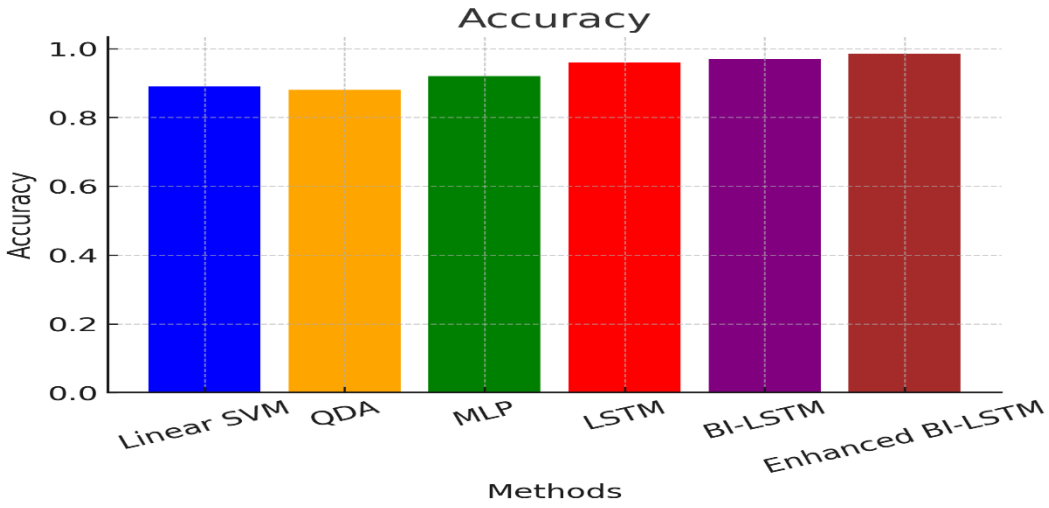

Figure 4. Accuracy of Enhanced BI-LSTM with existing models.

The accuracy figure 4 showcases the performance of different models in correctly classifying intrusions and normal traffic in the KDD Cup 1999 dataset. Enhanced BI-LSTM achieves the highest accuracy (98.5%), followed closely by

BI-LSTM (97%) and LSTM (96%). Traditional models like Multi-Layer Perceptron (MLP) and Linear SVM lag behind, highlighting the superiority of deep learning models in intrusion detection tasks.

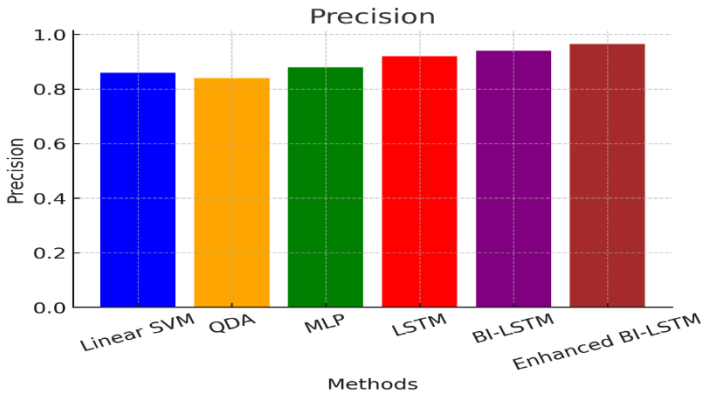

Figure 5. Precision of Enhanced BI-LSTM with existing models.

Precision measures the ability of a model to correctly classify positive instances (attacks) while minimizing false positives. The figure 5 indicates that Enhanced BI-LSTM (96.5%) and BI-LSTM (94%) outperform all other methods, reflecting their robustness in making correct attack predictions. Traditional classifiers like QDA and Linear SVM have lower precision, meaning they generate more false positives.

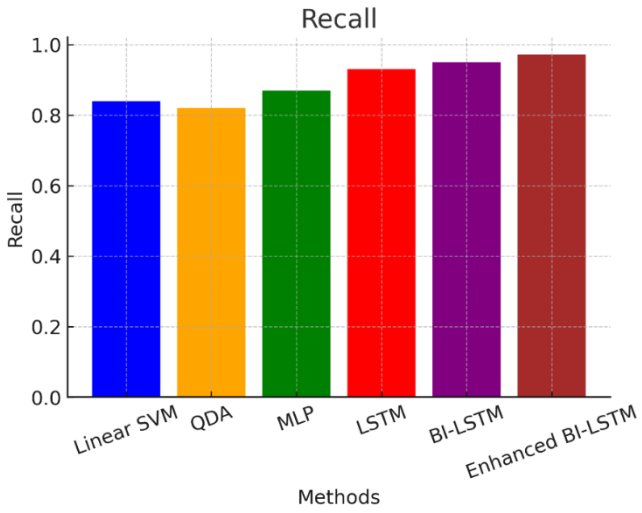

Figure 6. Recall of Enhanced BI-LSTM with existing models.

The recall figure 6 emphasizes the effectiveness of models in detecting all attack instances (true positives). Enhanced BI-LSTM (97.2%) achieves the highest recall, ensuring that nearly all attacks are detected, reducing false negatives. BI-LSTM and LSTM also perform well, whereas SVM and QDA have relatively lower recall values, meaning they miss more intrusions.

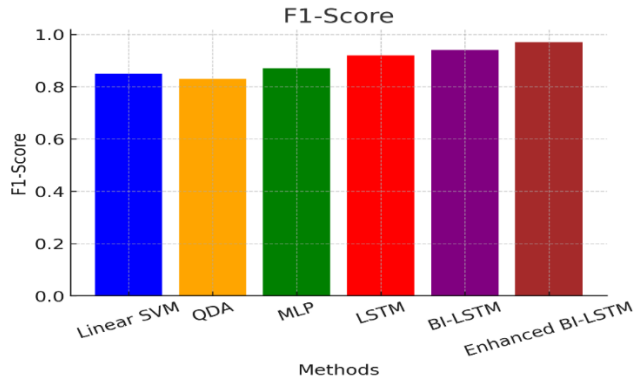

Figure 7. F1-score of Enhanced BI-LSTM with existing models.

The F1-score is the harmonic mean of precision and recall, balancing the trade-off between false positives and false negatives. The figure 7 shows that Enhanced BI-LSTM (97%) has the best balance between precision and recall, followed by BI-LSTM (94%) and LSTM (92%). This confirms that deep learning models outperform traditional methods in handling intrusion detection complexities.

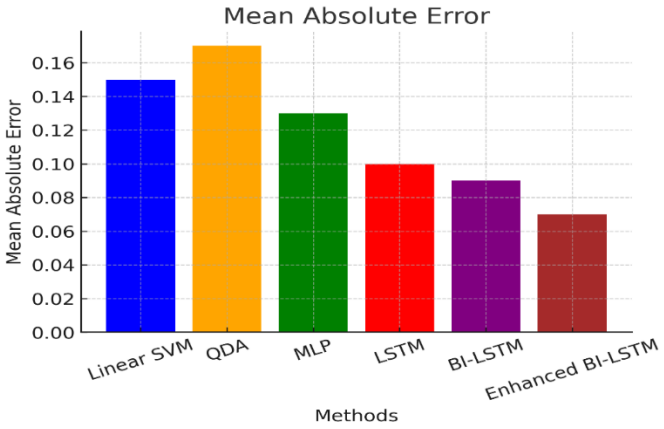

Figure 8. MAE of Enhanced BI-LSTM with existing models.

The figure 8 MAE represents the average absolute difference between predicted and actual values, with lower values indicating better performance. The graph shows that Enhanced BI-LSTM has the lowest MAE (0.07), meaning it makes fewer prediction errors. SVM and QDA have the highest MAE values (0.15 and 0.17, respectively), showing that their predictions deviate significantly from actual labels.

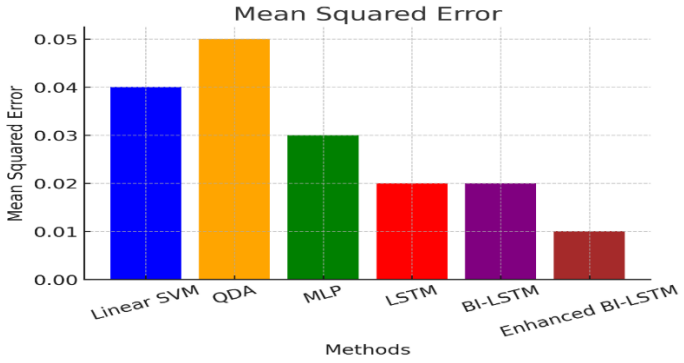

Figure 9. MSE of Enhanced BI-LSTM with existing models.

The figure 9 MSE penalizes larger errors more than smaller ones, making it a crucial metric for evaluating model reliability. Enhanced BI-LSTM has the lowest MSE (0.01), demonstrating its precision in detecting intrusions. Traditional models like QDA and SVM exhibit higher MSE values (0.05 and 0.04, respectively), indicating more frequent and larger prediction errors.

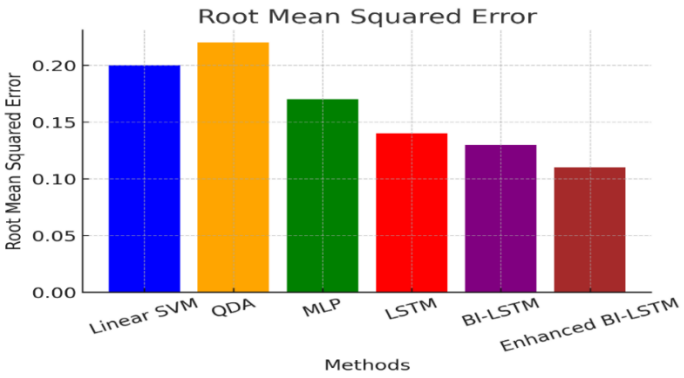

Figure 10. RMSE of Enhanced BI-LSTM with existing models.

RMSE is the square root of MSE, providing an error metric in the same unit as the predicted variable. The figure 10 highlights that Enhanced BI-LSTM (0.11) and BI-LSTM (0.13) have the lowest RMSE values, ensuring greater accuracy in intrusion detection. SVM and QDA have significantly higher RMSE values (0.20 and 0.22, respectively), showing that they generate higher deviations in predictions.

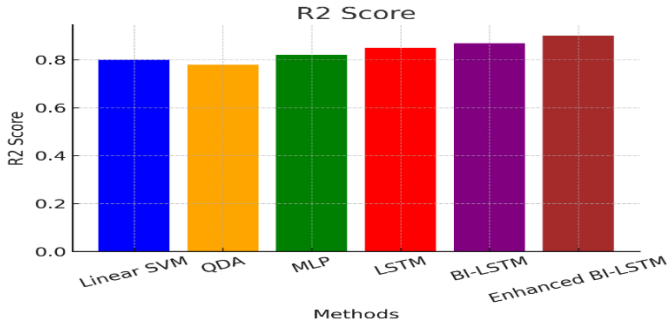

Figure 11. R^2 score (coefficient of determination) of Enhanced BI-LSTM with existing models.

The R^2 score (coefficient of determination) measures how well the model explains variance in the dataset. The figure 11 indicates that Enhanced BI-LSTM (0.90) has the highest R^2 score, suggesting it captures nearly all variance in intrusion detection. BI-LSTM (0.87) and LSTM (0.85) also perform well, whereas traditional models like QDA and SVM have lower R^2 scores (0.78 and 0.80, respectively), meaning they explain less variance and are less reliable.

5. CONCLUSION

This study demonstrates the effectiveness of the Enhanced BI-LSTM model for intrusion detection, integrating Feature Selection, Attention Mechanism, and Regularization to optimize network security. The model's application on the KDD Cup 1999 dataset shows significant improvements over traditional machine learning and deep learning methods, achieving 98.5% accuracy with lower Mean Absolute Error (MAE) and Root Mean Squared Error (RMSE). The incorporation of PCA and Chi-Square feature selection reduces computational complexity, while the Attention Mechanism enhances learning efficiency. These enhancements result in superior intrusion detection accuracy and fewer false alarms, making the model highly suitable for real-world cybersecurity applications. Future work will focus on scalability, real-time detection, and performance evaluation on modern intrusion datasets.

REFERENCES

[1] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, “Anomaly-based intrusion detection system for IoT networks through deep learning model,” *Computers and Electrical Engineering*, vol. 99, p. 107810, 2022.

[2] T. S. Naseri and F. S. Gharehchopogh, “A feature selection based on the farmland fertility algorithm for improved intrusion detection systems,” *Journal of Network and Systems Management*, vol. 30, no. 3, p. 40, 2022.

[3] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, “A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network,” *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55-68, 2022.

[4] W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, and M. Portmann, “E-graphsage: A graph neural network-based intrusion detection system for IoT,” in *NOMS 2022 - 2022 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2022, pp. 1-9.

[5] S. Neupane et al., “Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities,” *IEEE Access*, vol. 10, pp. 112392-112415, 2022.

[6] E. Caville, W. W. Lo, S. Layeghy, and M. Portmann, “Anomal-E: A self-supervised network intrusion detection system based on graph neural networks,” *Knowledge-Based Systems*, vol. 258, p. 110030, 2022.

[7] G. Apruzzese, M. Andreolini, L. Ferretti, M. Marchetti, and M. Colajanni, “Modeling realistic adversarial attacks against network intrusion detection systems,” *Digital Threats: Research and Practice (DTRAP)*, vol. 3, no. 3, pp. 1-19, 2022.

[8] S. Agrawal et al., “Federated learning for intrusion detection system: Concepts, challenges and future directions,” *Computer Communications*, 2022.

[9] N. Wang et al., “MANDA: On adversarial example detection for network intrusion detection system,” *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1139-1153, 2022.

[10] V. Ravi, R. Chaganti, and M. Alazab, "Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system," *Computers and Electrical Engineering*, vol. 102, p. 108156, 2022.
[11] Q. Abu Al-Haija and A. Al Badawi, "High-performance intrusion detection system for networked UAVs via deep learning," *Neural Computing and Applications*, vol. 34, no. 13, pp. 10885-10900, 2022.
[12] D. N. Mhawi, A. Aldallal, and S. Hassan, "Advanced feature-selection-based hybrid ensemble learning algorithms for network intrusion detection systems," *Symmetry*, vol. 14, no. 7, p. 1461, 2022.
[13] R. Chaganti et al., "A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things," *Sustainability*, vol. 14, no. 19, p. 12828, 2022.
[14] R. Balaji et al., "Survey on intrusions detection system using deep learning in IoT environment," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Apr. 2022, pp. 195-199.
[15] T. T. H. Le, Y. E. Oktian, and H. Kim, "XGBoost for imbalanced multiclass classification-based industrial internet of things intrusion detection systems," *Sustainability*, vol. 14, no. 14, p. 8707, 2022.
[16] E. E. Abdallah and A. F. Otoom, "Intrusion detection systems using supervised machine learning techniques: A survey," *Procedia Computer Science*, vol. 201, pp. 205-212, 2022.
[17] M. A. Almaiah et al., "Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels," *Electronics*, vol. 11, no. 21, p. 3571, 2022.
[18] M. Zipperle, F. Gottwalt, E. Chang, and T. Dillon, "Provenance-based intrusion detection systems: A survey," *ACM Computing Surveys*, vol. 55, no. 7, pp. 1-36, 2022.
[19] Y. B. Abushark et al., "Cyber security analysis and evaluation for intrusion detection systems," *Computers, Materials & Continua*, vol. 72, pp. 1765-1783, 2022.
[20] T. Zebin, S. Rezvy, and Y. Luo, "An explainable AI-based intrusion detection system for DNS over HTTPS (DoH) attacks," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2339-2349, 2022.
[21] Z. Lin, Y. Shi, and Z. Xue, "IDSGAN: Generative adversarial networks for attack generation against intrusion detection," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, May 2022, pp. 79-91.
[22] S. T. Mehedi et al., "Dependable intrusion detection system for IoT: A deep transfer learning-based approach," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1006-1017, 2022.
[23] M. Chalé and N. D. Bastian, "Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems," *Expert Systems with Applications*, vol. 207, p. 117936, 2022.
[24] M. A. Haq, M. A. R. Khan, and T. AL-Harbi, "Development of PCCNN-based network intrusion detection system for EDGE computing," *Computers, Materials & Continua*, vol. 71, no. 1, 2022.