Volume (1) No (11), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

A Unified Learning Strategy for Intrusion Identification in Intelligent Cyber-Physical Systems

Dr. Nilesh Jain
Associate Professor
Department of Computer Science and Applications
Mandsaur University
Mandsaur, India
nileshjainmca@gmail.com

***Abstract*—There is an increasing requirement to identify attacks against Cyber-Physical Systems (CPSs) due to their increasing application in critical infrastructures. Despite perhaps depending on sophisticated machine learning (ML) and deep learning (DL) models, the majority of intrusion detection techniques do not take practical implementation into account. This study uses the Knowledge Discovery and Data Mining Cup 1999 (KDDCup99) dataset to develop a novel hybrid deep learning (DL) model for the reliable detection of intrusions in Smart Cyber-Physical Systems (CPSs). The Synthetic Minority Oversampling Technique (SMOTE) is used to address the problem of class imbalance after the dataset has been cleaned, noise-reduced, fitted with outliers eliminated, and normalized using the Z-score. The main innovation is that it blends the temporal sequence modeling of bidirectional long short-term memory (BiLSTM) with the spatial feature-originating of convolutional neural networks (CNNs). The model's ability to capture both sequential and structural attack patterns is made possible by its synergy. With a score of 99.9% on every metric, including F1-score (F1), recall (REC), accuracy (ACC), and precision (PRE), the model achieves exceptionally good results. When compared to more conventional machine learning models like Support Vector Machine (SVM), K-Means Clustering (K-Means) + Random Forest (RF), and a simple CNN, the superiority of the suggested hybrid model is demonstrated. Because of its exceptional generalization and adaptability, it is most appropriate for real-time intrusion detection in the intricate and dynamic Cyber-Physical System (CPS) environment. The potential advantages of hybrid DL in improving the security and resilience of vital smart systems are discussed in this study.**

Keywords*—Cyber-Physical Systems (CPS), Intrusion Detection Systems (IDS), Hybrid Deep Learning, Spatial Feature Extraction, Network Security, Real-Time Detection.

I. INTRODUCTION

The quantity of private information on Internet usage has increased in tandem with network-related service usage. Intruders are unauthorized users who seek to breach a system or take confidential data with malevolent intent. Even with a variety of network security techniques, cyberattacks continue to occur. Since network infiltration is a major threat, NIDSs are required to stop these kinds of attacks. To identify similar attacks in the future, the knowledge gathered by examining the packet data during assaults might be useful [1][2][3]. Network activity monitoring and security breach detection depend heavily on IDS. In terms of identifying new and advanced threats, most signature-based techniques employed by traditional IDS have drawbacks [4][5]. Computer networks are protected by IDS, which recognizes and addresses security threats.

Cyber-Physical Systems (CPSs) are the foundation of many essential aspects of everyday existence. Attacks might result in harm to tangible items, assets, and those who rely on CPSs because the majority of them are safety-critical [6][7][8]. Over time, the scientific community has been more concerned about protecting CPSs against attacks and threats. CPSs must be robust, which means they must function through incidents and deal with their fallout. By accepting occurrences through online detection and reaction, resilience may be attained [9]. The main defences against outside threats for CPS devices are firewalls, antivirus software, and encryption. These defences, however, are unable to completely prevent attacks, particularly since attackers are always changing their tactics.

The foundation of smart city configurations is cyber-physical systems. A smart city is not universally defined. Its connotation varies depending on the location. Every nation has a different idea of what a smart city should look like. It differs from nation to nation, city to city, and location to location [10][11]. Every nation has a unique combination of needs and capacities, which influences its perspectives and readiness to change. This is seen in the shift from traditional city layouts to urban smart city settlements.

A possible strategy to better safeguard systems and networks is to utilize machine learning (ML) models for identifying new attack types and for real-time anomaly detection (AD). An ML-based study on the contamination strategies used to target CPS deployments uses big data analysis to identify patterns that indicate illicit activities [12][13]. These complex anomaly detection systems are generated by supervised learning, unsupervised learning and reinforcement learning among the many techniques that are used [14]. As an illustration, supervised learning algorithms that can differentiate between typical and aberrant behavioral patterns can be quickly trained using tagged data.

A hybrid deep learning (DL) algorithm [15][16][17] is used to formulate a new IDS developed in large data scenarios. This approach enables detection of the emerging and existing cyberthreats accurately and efficiently. The benefits of extracting the temporal patterns using BiLSTM networks and

the spatial data using CNNs. The proposed solution exploits scalable architecture, advanced pre-processing, and SMOTE imbalance processing to handle the big amount of information, velocity and diversity of big data. It works best in the real-time monitoring of threats in complex networked systems.

A. Background of the Study

A cyber-physical system (CPS) is used in most intelligent communication and networking applications to control and monitor physical systems. Because of their superior capabilities, flexibility, scalability, and security concerns above the basic embedded systems now in use, these applications call for advancements in CPS. Identifying various risks and assaults and stopping them from infecting the system are both essential components of information security in cyber networks. Both established and new CPSs can use IDS and IPS to protect their data. Hybrid strategies were created to improve detection methods that relied on pattern comparison in smart intrusion detection and prevention systems. A method for conducting penetration tests or assessing the robustness of the established security protocols is vulnerability analysis. Security professionals use threat modelling to identify system vulnerabilities that might pose a danger and create countermeasures. Together with other created security mechanisms, these two methods are fundamental and necessary components of security processes utilized in both legacy and contemporary security solutions that are taken into consideration in CPSs.

B. Motivation and Contribution of the Study

The blending of physical and cyber space in Smart Cyber-Physical Systems (CPS) has transformed many sectors, including industrial control and healthcare, providing unprecedented automation and efficiency. Such systems are highly susceptible to advanced attacks due to the emergence of fresh and complex security vulnerabilities through their interconnectivity. Traditional IPS are often used to attack conventional IT networks. The urgency of the effective and advanced IDS capable of effectively safeguarding the integrity of information is what drove this work, availability, and confidentiality of smart CPS, and the alleviation of the potentially devastating effects of successful attacks on the critical infrastructure and the further safe and reliable operation of these critical services. The main contributions of this work are the following:

- Recent and famous KDDCup99 dataset utilized at Kaggle.
- Large-scale data preparation processes were conducted to ensure that the input of the model is of high quality, such as data cleaning, outlier fitting, noise reduction, and Z-score normalization.
- Used the SMOTE for the effective balancing of the dataset with numerous classes.
- A new hybrid DL architecture was created and implemented with CNN and BiLSTM to augment the process of detecting sequential patterns and features of network traffic data.
- evaluated the suggested CNN+BiLSTM model's performance in-depth using a number of criteria, including REC, ACC, PRE, F1, and loss.

C. Novelty and Justification of the Study

In this paper, a novel IDS is proposed, which integrates CNN with BiLSTM networks with Smart CPS in particular. The main novelty is the synergistic combination of CNNs to extract spatial patterns of high-dimensional network traffic and BiLSTMs to model bidirectional time dependencies and allow the more comprehensive representation of dynamic CPS environments. The methods like data pre-processing and SMOTE are individually developed, but their combined optimization in terms of inclusion into this hybrid deep learning network of CPS security is not previously tested. The temporal and complex nature of CPS traffic often leads to poor performance and falseness of conventional intrusion detection systems. The proposed CNN-BiLSTM model addresses these concerns by enhancing the real-time statement of complicated attack vectors and slight anomalies. The strategy is particularly justified in the case of CPS, where an immediate and accurate threat detection is critical, which provide better ACC, PRE, and REC and consume less resources in resource-limited conditions.

D. Structure of the Paper

The structure of the paper is as follows: The pertinent literature review on intrusion detection in smart cyber-physical systems is given in Section II; the technique is described in Section III; the results and model comparisons are presented in Section IV; and the conclusions and research recommendations are outlined in Section V.

II. Literature Review

This section reviews the literature on intrusion detection in intelligent cyber-physical systems. Most research highlights the application of various methods to improve work scheduling effectiveness in cloud systems. Common themes emerging from the reviewed literature include:

Hussein, Hammood and Al-Abbasi (2025) proposed a new IDS called Deep Cyber-IDS is discussed, which addresses these issues by using DL to spot complex network traffic patterns and requires less fine-tuning or creation of new features. The system combines CNN, GRU, and LSTM layers to draw useful information from the raw traffic data in terms of space and time. The Deep Cyber-IDS system is unique among IDS designs as it can learn from its own input data, which enables it to adjust to the different circumstances on the network without any outside interference. It was implemented on three popular datasets that are commonly used to identify its effectiveness. NSL-KDD, UNSW-NB15 and Smart Grid. The model scored a perfect F1 on UNSW-NB15 and Smart grid, as well as a PRE and REC of 100 and an ACC of 99,84% on NSL-KDD [18].

Dayarathne et al. (2025) emphasized employing the DL architectures, i.e. CNN and LSTM networks, to rapidly detect grid data abnormalities. The models that have been designed based on the simulated cyberattacks and PSCAD simulated data have significantly enhanced threat identification and mitigation. This research paper identifies the difficulties that come with detecting cyber threats in grids with high proportions of renewable energy such as the frequency instability or lower inertia and suggests more sophisticated forecasting and energy storage methods to address the problem. The pre-processing technique that is unique and incorporated in the suggested models to identify cyber risks using feature derivatives enables them to identify cyber risks with 98% ACC or more, which is a powerful framework to mitigate smart power grids against the emerging threats [19].

Rajathi et al. (2024) proposed an AIDS based on reinforced learning (RL)-based Autoencoders (AE) that enables the possibility of recognizing and managing cyber-attacks in CPS scenarios. This proposed model combines the process of autoencoders in the unsupervised learning sphere and the process of reinforcement learning to continuously refresh the model and increase its ACC. Findings on benchmark CPS data show that RL-AE-based IDS is able to reduce the rate of false positives to 2.4% with a detection rate of 98.3%, a PRE rate of 96.8% and a REC rate of 97.5%. The system also proved to be very fast to adapt with less than 50 iterations to address new attack patterns. These findings point to the model's capacity to boost system resilience and enable the safe and efficient operation of critical infrastructure scenarios [20].

J, M and S (2024) proposed an intrusion-type typology to identify cyberattacks on the modern smart power systems, which combine multi-area power systems. It employs Hybrid Res2-UNeXt and a federated learning-based optimization algorithm to learn complicated electrical grid characteristics. DL, coupled with federated learning is an effective way to identify and frame intrusions thus boosting the securities of smart grids. The proposed method achieved 96.6% ACC when analysing the original set of features and delivered a maximum ACC of 99% with the selected dataset from the publicly available dataset at Mississippi State University. Therefore, the suggested intrusion categorization method might successfully defend smart power grid systems from online threats [21].

Latha and Bommi (2023) suggested that a huge amount of secret information, exchange information, exercises and subsequent meetings are transferred to the organization in current days through basic advances. Thus, it is become adaptable for end clients to transfer the information securely over the cloud beyond intrusion attacks. Each time the client logs in to the specific organization, empower the authorized person to access nodes, to acknowledge every access to the contributions for a specific timeframe. In order to identify network intrusions that affect IoT devices, the suggested approach seeks to offer a reliable model. The IDS2017 dataset is used by the system to create a Cat Boost regression model. The approach being presented considers several factors as critical factors for identifying whether intrusion attacks are occurring on the network. The system's ACC was 92.5%, and it was contrasted with other cutting-edge techniques [22].

Ahmed, Jeon and Ahmad (2023) controller area network (CAN), a basic method for managing communication between several in-vehicle network sensors, is advised for use in contemporary automobiles. There are insufficient security mechanisms in place to enable data encryption, authorisation, and authentication processes in order to defend the network against hostile invasions include denial of service and fuzzy attacks. In this study, a DL-based IDS for safeguarding the CAN bus in automobiles is proposed. Malicious assaults are identified by using and training the VGG architecture to detect different network intrusion patterns. The CAN intrusion dataset is used to conduct the tests. When compared to traditional ML methods, the experimental results show that the false positive rate (FPR) is considerably decreased by the suggested DL method. The system's FPR is 0.6% and its total ACC is 96% [23].

Abdullahi et al. (2022) CPS vulnerable to serious cyberattacks. This calls for novel DL techniques that are able to identify, look into, query, and react to variations in these types of assaults. This paper suggested an LSTM-based DL model to detect cybersecurity vulnerabilities in the CPS. Additionally, real data sets from the ICS of gas pipelines, which comprise 19 attributes and seven different attack types, were used to evaluate the model. Following validation, the experiment's findings show that the suggested model's ACC was 98.22%. The study also includes a proposal that might be implemented in the future [24].

Vedant et al. (2022) since there are more smart device accesses and information exchanges than in any preceding single-structured system, CPPS is more vulnerable to attacks. The cyber subsystem may be exploited by hackers and malware to target the CPPS, which could be detrimental to the actual energy transmission system. The essay concentrates on recognising and detecting cyberattacks on the CPPS while keeping this in mind. The author of the research proposes that, with the use of a DT, an IDS might be implemented to recognize the different types of cyberattacks employed against the CPPS. The computation of evaluation metrics such as ACC, PRE, REC, and F1, utilising a variety of attack types demonstrates the value of the suggested IDS [25].

The analysis of bac papers in terms of their background study regarding Methodology, Dataset/Environment, Problem Addressed, Performance and Future Work/Limitation is presented in Table I.

TABLE I. REVIEW OF LITERATURE ON INTRUSION DETECTION IN SMART CYBER-PHYSICAL SYSTEMS

Author(s)	Methodology	Environment	Performance	Future Work / Limitation
Hussein, Hammood and Al-Abbasi (2025)	DeepCyber-IDS using CNN, GRU, and LSTM for spatio-temporal analysis of raw traffic data	NSL-KDD, UNSW-NB15, SmartGrid	100% precision and recall on UNSW-NB15 & SmartGrid; 99.84% accuracy on NSL-KDD	Less emphasis on feature engineering; further generalization to more network environments recommended
Dayarathne et al. (2025)	CNN and LSTM with novel feature derivative-based preprocessing	PSCAD-simulated smart grid with synthetic attacks	>98% accuracy in anomaly detection	Requires validation on real-time or real-world smart grid data with high renewable energy integration
Rajathi et al. (2024)	Reinforcement learning-based autoencoders (RL-AE) for adaptive intrusion detection	Benchmark CPS datasets	98.3% accuracy, 96.8% precision, 97.5% recall; <50 iterations convergence	Needs scalability assessment and multi-agent deployment capability
J, M and S (2024)	Hybrid Res2-UNeXt with federated learning for smart grid intrusion classification	Multi-area smart grid (Mississippi State Univ. dataset)	96.6% accuracy (original), 99% (selected features)	More interpretability and real-time federated updates needed
Latha and Bommi (2023)	CatBoost Regression-based IDS using key attributes for intrusion detection	IDS2017 dataset; IoT environment	92.5% accuracy	Limited to regression-based models; potential enhancement via hybrid or ensemble models

Ahmed, Jeon and Ahmad (2023)	VGG-based deep learning model for CAN bus security in smart vehicles	CAN-Intrusion Dataset (Vehicle networks)	96% accuracy, 0.6% FPR	Focused on CAN; future work includes extending to other vehicle network types
Abdullahi et al. (2022)	LSTM-based deep learning IDS for ICS environment	ICS datasets (Gas pipeline)	98.22% accuracy	Limited feature space; suggests exploring hybrid DL architectures and more diverse datasets
Vedant et al. (2022)	Decision Tree-based IDS for cyber-physical production systems (CPPS)	CPPS with frequent device interactions	Metrics computed: accuracy, precision, recall, F1-score	Decision tree limitations with high-dimensional data; recommends DL or ensemble approaches

III. Methodology

The given section outlines an intrusion detection process, beginning with Kaggle-downloaded KDDCup99 data. The most crucial step of data pre-processing, which includes data cleaning, outlier fitting, noise reduction, and Z-score normalization to guarantee data quality, is next applied to this raw data. The data is then balanced using the SMOTE, particularly the multiclass classifications. After balancing, this data is divided into training, assessment, and testing sets. The CNN+BiLSTM model categorization is the primary concept of the given system. The measures of loss, F1, REC, ACC, and PRE are then used to critically assess the model's performance. The process's output is the final result. Figure 1 illustrates the proposed methodology flowchart of intrusion detection.

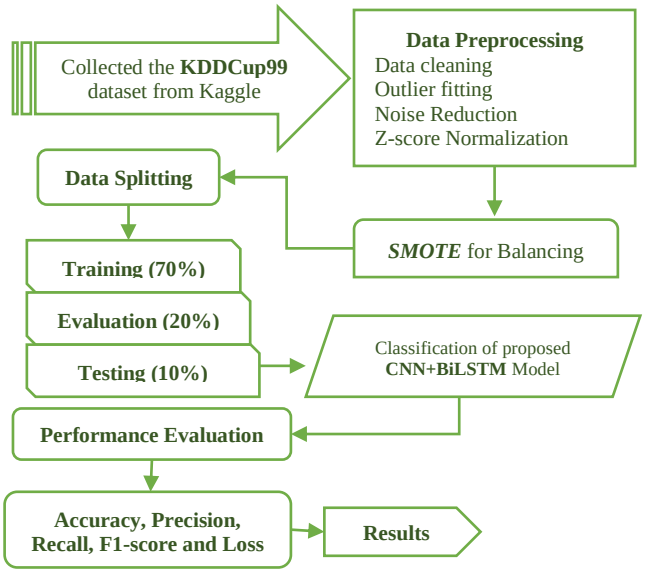

Fig. 1. Flowchart of Intrusion Detection in Smart Cyber-Physical Systems

Each step of the flowchart is explained in the section below:

A. Data Collection

The KDDCup99 dataset from Kaggle was utilized in this investigation. This dataset was used in the Third International Knowledge Discovery and Data Mining Tools Competition, which was sponsored by KDD-99, the Fifth International Conference on Knowledge Discovery and Data Mining. Developing a prediction model that could distinguish between "bad" connections, often referred to as incursions or assaults, and "good" regular connections was the competition's objective. A variety of simulated intrusions in a military network environment are occasionally used in this database's audited data collection. Below in this section are several Exploratory Data Analysis (EDA) graphs:

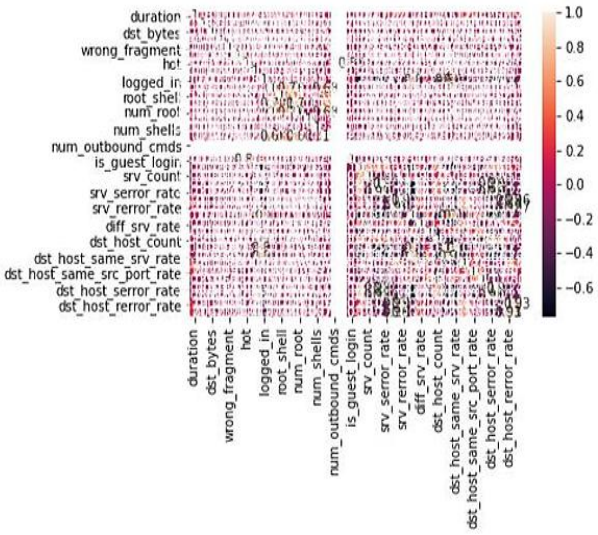

Fig. 2. Correlation of all features

Figure 2 presents a heatmap of the correlation matrix for features from a network intrusion detection dataset. The colour scale ranges from -1 (dark) to 1 (light), indicating the degree and orientation of linear correlations between characteristics. Lighter shades represent strong positive correlations, darker shades indicate negative correlations, and mid-tones suggest weak or no correlation. Although the correlation values are included, they are difficult to read due to the dense layout. This visualization supports feature selection and dimensionality reduction by aiding in the detection of traits that are redundant or closely related.

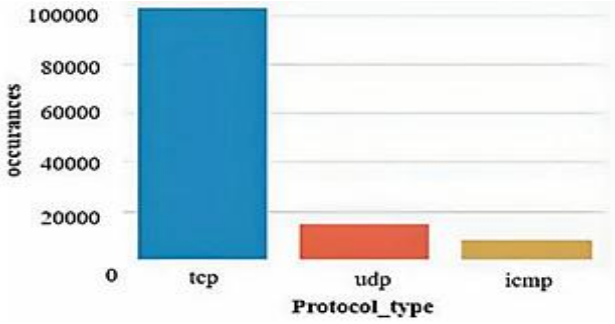

Fig. 3. Categorical Feature protocol_type *vs.* occurrences

The distribution of the dataset's network protocols according to their frequency of occurrence is shown in Figure 3. TCP records the largest number of incidents by far of the three types of protocols of UDP, ICMP, and TCP almost 100,000. UDP and ICMP are much lower, and relatively similar, at approximately less than 20,000. It means that the most common traffic in the dataset is TCP which is common in most network environments in reality as it is reliable and used extensively in internet traffic.

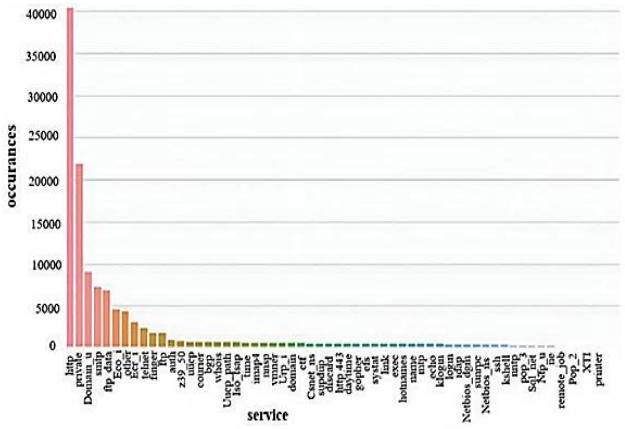

Fig. 4. Categorical feature service vs. occurrences

Figure 4 illustrates distribution of different network services in the data set. The most repeated service is the one called http (almost 40,000 times), and the next group in order of descending frequency is the service called private and the service called domain u (about 20,000 times each). There is a noticeable long-tail distribution with few services of high frequencies and many of the services are infrequent. Such skewed distribution has the implication that network traffic is highly concentrated around few common services, a characteristic feature of network usage patterns, and is useful in detecting anomalies or attacks on less common services.

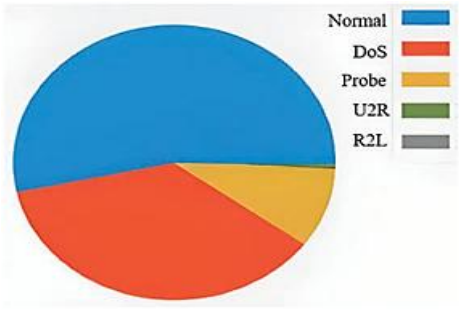

Fig. 5. Attack type *vs.* normal

Figure 5 shows the network traffic distribution in five categories, including the normal, DoS, Probe, U2R, and R2L. The dataset is dominated by normal traffic (blue) with a large proportion of DoS attacks (red) thereafter. Probe attacks (yellow) are less frequent, while U2R (green) and R2L (Gray) appear rarely. The graph highlights a notable class disparity, with Normal and DoS traffic making up the majority.

B. Data Preprocessing

Here, the variables that remained after lowering correlations were pre-processed using a methodical approach, in which each variable was analysed separately and the most effective method was employed. The steps for data pre-processing are discussed below likely outlier fitting, noise reduction and z-score normalization:

- **Data Cleaning:** The practice of fixing or removing inaccurate data from a data file is known as data cleaning, which includes processing erroneous or missing values and detecting the data's rationality—that is, replacing, changing, and removing the dirty data.
- **Outlier Fitting:** In order to identify outliers in a variable, plotting over time to emphasize values that diverge from the signal's overall trend or displaying values further from the mean requires a histogram [26]. Programmatically, numbers that fall inside a certain range are removed in order to eliminate outliers.
- **Noise Reduction:** A linear filter is a useful tool for reducing or eliminating noise. This study used three filters: a one-dimensional digital filter, a median filter, and a Gaussian-weighted moving average filter [27]. The variable must be visualized before choosing a filter, and the kind of filter chosen must be determined by the intended outcome.
- **Z-score Normalization:** A crucial feature scaling technique is standardization, also referred to as z-score normalization. The result is divided by the standard deviation after deducting the average value of each attribute [28]. This method works particularly well when the input data has a significant variation in feature values. Equation (1) provides the Z-score normalization's mathematical form:

$$x_{new} = \frac{x-\mu}{\sigma} \quad (1)$$

In the above Equation (1), x stands for the original feature value, x_{new} for the standardised value, μ for the original feature mean, and σ for the original feature standard deviation.

C. Synthetic Minority Over-Sampling Technique (SMOTE) for Balancing

SMOTE uses an oversampling approach to enhance the minority classes by generating fresh samples using an interpolation procedure. Before being used to create new minority class samples, the detected minority samples are pooled together. Instead of reproducing minority samples, SMOTE creates synthetic samples [29]. The issue of imbalanced datasets and potential overfitting was resolved by using SMOTE. The method enhanced the model's generalization by ensuring that the dataset contained a balanced representation of both normal and incursion examples.

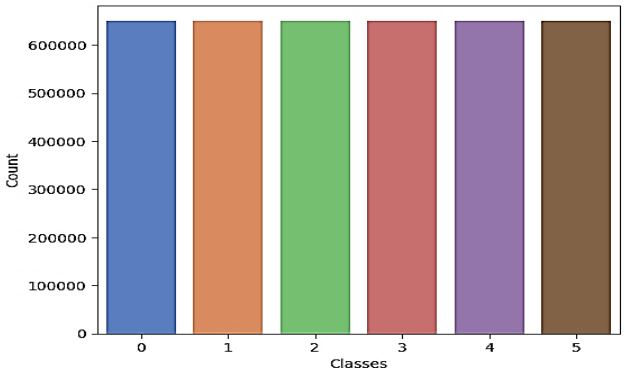

Fig. 6. Data distribution after applying SMOTE for

The class distribution of the dataset utilized for intrusion detection is depicted in Figure 6, which displays a balanced representation across all six classes, designated 0 through 5. Each bar corresponds to a specific class and displays a nearly identical count, approximately exceeding 600000 instances per class. This uniform distribution indicates that building trustworthy ML and DL models requires a well-balanced dataset. Balanced class representation helps prevent model bias toward any particular class and contributes to more accurate and generalizable intrusion detection performance.

D. Data Splitting

To prepare it for IDS, the KDDCup-99 dataset needs to be divided into distinct files. Consequently, throughout the data-splitting process, the test, evaluation, and training sets are 70%, 20%, and 10% isolated from the entire data set, respectively.

E. Proposed Hybrid CNN-BiLSTM Model

Traditional IDS, which typically employ rule-based systems or shallow ML models, may find it difficult to handle the dynamic nature of assaults and the resource limitations of IoT devices with restricted capabilities. To overcome these obstacles, present a unique hybrid model that combines the advantages of BiLSTM layers with IoT networks can effectively identify intrusions using lightweight CNNs. A lightweight CNN architecture is used in the initial phase of the model, which is specifically made for effective processing on edge devices [30][31]. In comparison to conventional CNNs, this CNN employs fewer layers and parameters, which reduces memory usage and computational complexity without compromising usable ACC. To find patterns and connections among multiple data points, the network traffic data's geographical information is utilized by the convolutional layers.

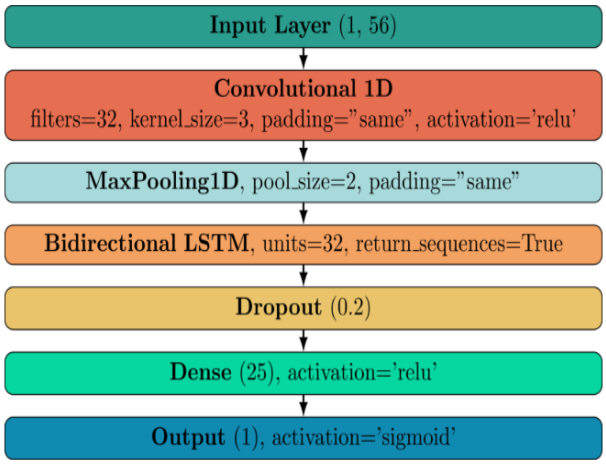

Fig. 7. The architecture of Lightweight CNN-BiLSTM Model

The characteristics are then recovered and sent to in sequential data, a BiLSTM layer is very good at identifying temporal correlations. The suggested CNN-BiLSTM model architecture is shown in Figure 7. Given that cyberattacks frequently display distinct patterns over time, this is very helpful for network traffic analysis. Through feature sequence analysis, the BiLSTM detects anomalies that diverge from typical network activity and reveals the underlying dynamics [32][33]. Utilizing the advantages of both methods, the CNN and BiLSTM layer findings are integrated. A sigmoid classifier, which evaluates whether network traffic is malicious or normal, is one of the last decision-making layers that receives the combined information. The two LSTM components that make up the BiLSTM model. The input sequence is processed by two LSTM units, one of which moves forward and the other backward. The forward LSTM in Figure 8 evaluates the input sequence from start to finish, while the reverse LSTM does the opposite. The final hidden state sequence is produced at each time step by concatenating or combining the hidden states of the two LSTMs. The following layer then receives this concatenated sequence. Equations (2) to (4) offer a mathematical depiction of this process:

$$h_t^{(f)} = LSTM^{(f)}(x_t, h_{t-1}^{(f)}, c_{t-1}^{(f)}) \quad (2)$$

$$h_t^{(b)} = LSTM^{(b)}(x_t, h_{t+1}^{(b)}, c_{t+1}^{(b)}) \quad (3)$$

$$h_t = [h_t^{(f)}; h_t^{(b)}] \quad (4)$$

where $h_t^{(f)}$ and $h_t^{(b)}$, respectively, represent the hidden forward and backward states at time step t. The forward and backward states of the cell at time step t are represented by c$c_{t-1}^{(f)}$ and $c_{t-1}^{(b)}$, respectively. x_t. represents an input vector at time step t. The forward and backward hidden states were concatenated to generate a single vector, represented by h_t.

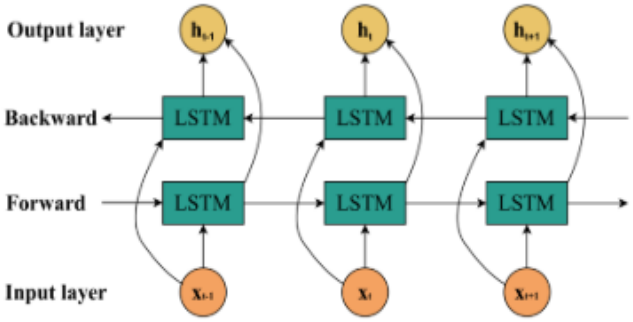

Fig. 8. BiLSTM architecture

F. Performance matrix

The performance of the IDS in smart cyber-physical systems could be improved by choosing the most relevant features and removing irrelevant ones or those that could present the same information [34]. Metrics are employed to evaluate IDS efficacy, the success (or failures) of IDS, when detecting or preventing the occurrence of a network or system intrusion and security breaches. Some typical IDS evaluation metrics are given below:

- **True Positives (TP):** This is the precise number of assaults or intrusions that the smart cyber-physical systems' IDS has been able to detect.
- **False Positives (FP):** It is the quantity of routine operations that the IDS in smart cyber-physical systems incorrectly interprets as intrusions or assaults. Another name for it is a false alarm.
- **True Negatives (TN):** This is the quantity of regular or harmless network activity that the intelligent cyber-physical systems' IDS accurately identified.
- **False Negatives (FN):** The IDS in smart cyber-physical systems failed to identify or categories this number of incursions or assaults as typical. "Missed detection" is another term for this.

These values are computed for each class individually during the testing phase, and they form the basis for calculating the evaluation metrics. These figures are utilized to generate the general formulas for F1, REC, ACC, and PRE.

1) Accuracy:

This is the proportion of instances that were successfully detected (TP + TN) to all occurrences. It presents in-depth evaluation of the accuracy of the IDS. The correctness of the overall model is calculated by means of Equation (5):

$$\text{Accuracy} = \frac{\text{TP+TN}}{(\text{TP+TN+FP+FN})} \quad (5)$$

2) Precision

The Precision can be determined as the percentage of TP to all the instances that the IDS is considered positive. It measures the prevention of false positives of the IDS. In Equation (6), the accuracy is taken into consideration:

$$\text{Precision} = \frac{\text{TP}}{(\text{TP+FP})} \tag{6}$$

3) Recall

This is the proportion of TP to the total positive cases. It evaluates the ability of the IDS to identify all positive incidences. Equation (7) shows the mathematical representation of the recall:

$$\text{Recall} = \frac{\text{TP}}{(\text{TP+FN})} \tag{7}$$

4) F1-Score

This represents the accuracy and recall harmonic mean. The quantity of FP and FN is balanced [35]. Equation (8) is used to calculate the F1-score:

$$\text{F}_1 - \text{Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}} \tag{8}$$

5) Loss Function

A loss function helps the model become more accurate by quantifying the discrepancy between expected and actual results. By reducing FP and FN, it is essential for improving detection performance and guaranteeing accurate, real-time threat identification.

IV. Results and Discussion

The tests were conducted on a Dell Desktop-CFDNAIN running 64-bit Windows 11 with a 2.00 GHz CPU and 64 GB of RAM. Using the Kera's and TensorFlow libraries, Python 3.7 was used to create the suggested hybrid DL models. To identify intrusions in smart CPS, Table II displays the evaluation metrics of the proposed hybrid CNN-BiLSTM model. With an F1, ACC, PRE, and REC of 99.9%, the model excels on all key criteria. Considering all of these high values, the model has very few FP and FN and is quite effective at correctly detecting both benign and malicious behaviour. These results demonstrate the model's strength, soundness, and great generalizability in detecting intrusion in complex cyber-physical contexts.

TABLE II. Evaluation of Hybrid Model on Intrusion Detection in Smart Cyber-Physical Systems

Metrics	CNN+BiLSTM
Accuracy	99.9
Precision	99.9
Recall	99.9
F1-Score	99.9

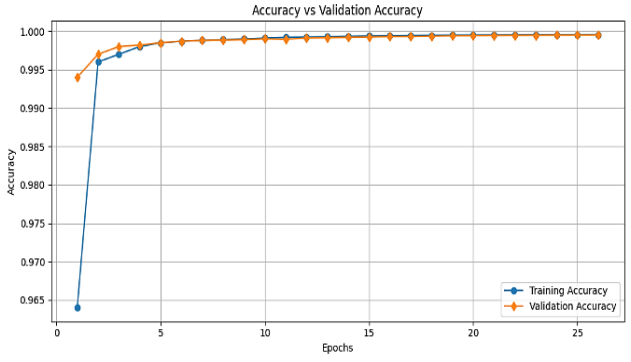

Fig. 9. Accuracy vs. Validation Accuracy of the Model

The ACC of the model over 26 epochs is displayed in Figure 9. Starting at 0.965, Training ACC (blue) rapidly increases to meet Validation ACC (orange), which starts close to 0.995. By epoch 5, both metrics stabilize close to 1.000, indicating convergence and outstanding results on training and validation data.

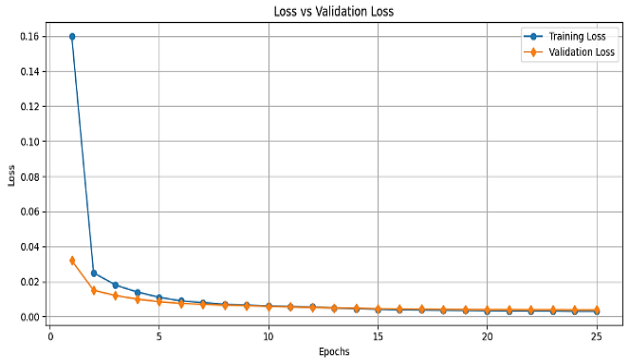

Fig. 10. Loss vs. Validation Loss of the Model

Figure 10 shows the model's loss over 25 epochs. Training Loss (blue) starts around 0.16 and drops sharply, while Validation Loss (orange) begins near 0.03 and also decreases rapidly. By epoch 15, both losses stabilize near zero, indicating effective learning and good generalization.

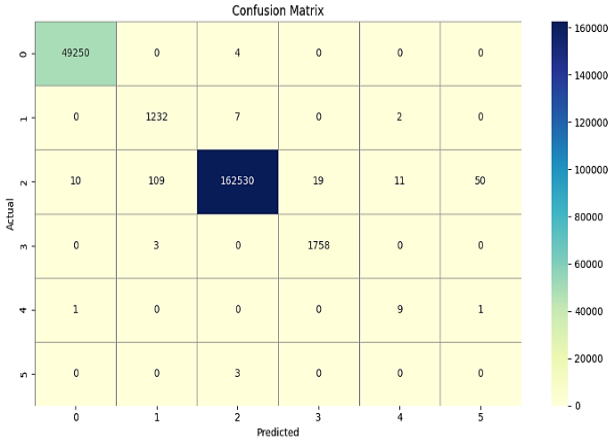

Fig. 11. Confusion Matrix of hybrid CNN-BiLSTM Classification performance on the KDD-Cup99 Dataset

A confusion matrix evaluating Figure 11 illustrates how well the model can classify data into six groups. Most predictions lie along the diagonal, indicating high ACC, especially for class 2 (162,530), class 0 (49,250), and class 3 (1,758). Misclassifications are minimal, with sparse off-diagonal values, reflecting strong model performance and effective class separation.

A. Comparative Analysis

The suggested CNN+BiLSTM model is compared against other ML and DL techniques in this section, CNN by itself, SVM, and K-Means in conjunction with RF. Several ML and DL models for intrusion detection in intelligent cyber-physical systems are compared in Table III. With an ACC of 99.9%, the CNN+BiLSTM hybrid technique outperforms the other models on the list, demonstrating its greater capacity to capture both spatial and temporal aspects of incursion patterns. The classical ML systems like the SVM have a high ACC of 97.15%, indicating their strength in the classification process. DL-based CNN achieves an ACC of 88% which

implies that it has moderate high flaws in extracting features of raw data. In the meantime, the ensemble model that consists of K-Means clustering and RF provides 85% ACC, which shows minimal efficiency in dealing with intrusion patterns. On the whole, the CNN+BiLSTM model performs better than others, proving the potential of hybrid DL models with regard to the improved intrusion detection in smart CPS conditions.

TABLE III. COMPARATIVE ANALYSIS OF ML AND DL MODELS ON INTRUSION DETECTION IN SMART CYBER-PHYSICAL SYSTEMS

Models	Accuracy
SVM [36]	97.15
CNN [37]	88
K-Means+RF [38]	85
CNN+BiLSTM	99.9

The CNN+BiLSTM model, which has been proposed for intelligent CPS intrusion detection, has a number of clear advantages. The model can recognize both dynamic and static patterns in the network traffic dataset thanks to the combination of CNN's capacity to extract spatial features and BiLSTM's capacity to learn temporal sequences. The architecture is based on two layers that allow the system to infer complex representations and dependencies that might be disregarded by single-models systems orientations. The hybrid CNN+BiLSTM model outperforms the conventional ML model, according to the comparative study. In addition to having high detection ACC, it also balances categorization with minimal false alarms, as demonstrated by its much-improved performance on every assessment criterion, including F1, REC, ACC, and PRE. These findings illustrate the strength, flexibility, and the ability of generalization of the model and as such, it is very effective in real time intrusion detection in complex and dynamic smart cyber-physical environment.

V. CONCLUSION AND FUTURE SCOPE

At the heart of Smart Cities implementation is coordination between the CPS, where different systems come together to accomplish shared objectives like sharing of resources, availability of data, and optimization of infrastructure components. In order to identify intrusions in Smart Cyber-Physical Systems, this research developed a new hybrid DL architecture that addresses the complexity and interconnection of these systems. The careful pre-processing of the KDDCup99 dataset and synergistic CNN-BiLSTM model architecture also allowed the research to develop a solid framework to distinguish malicious network traffic and benign traffic. In the designed model, the model's remarkable capacity to identify various intrusion types indicates that it has a great chance of being used in practical settings to secure critical CPS infrastructure. To build on this study in the future, it would be desirable to apply the study to more varied and up to date CPS data sets, perhaps having greater fidelity and being of a streaming nature. Additionally, exploring lightweight model architectures or distributed learning paradigms could be beneficial for deployment on resource-constrained CPS devices, in addition to researching explainable AI methods to increase the openness of the way the model makes decisions in crucial security situations.

REFERENCES

[1] S. Thakur, A. Chakraborty, R. De, N. Kumar, and R. Sarkar, "Intrusion detection in cyber-physical systems using a generic and domain specific deep autoencoder model," *Comput. Electr. Eng.*, vol. 91, May 2021, doi: 10.1016/j.compeleceng.2021.107044.

[2] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics : A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.

[3] N. Patel, "AI-Powered Intrusion Detection and Prevention Systems in 5G Networks," in *2024 9th International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Dec. 2024, pp. 834–841. doi: 10.1109/ICCES63552.2024.10859892.

[4] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, "Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity," 2023. doi: 10.3390/app13137507.

[5] R. P. Sola, N. Malali, and P. Madugula, *Cloud Database Security: Integrating Deep Learning and Machine Learning for Threat Detection and Prevention*. Notion Press, 2025.

[6] M. Catillo, A. Pecchia, and U. Villano, "CPS-GUARD: Intrusion detection for cyber-physical systems and IoT devices using outlier-aware deep autoencoders," *Comput. Secur.*, vol. 129, 2023, doi: https://doi.org/10.1016/j.cose.2023.103210.

[7] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. 3, 2025, doi: 10.47001/IRJIET/2025.903027.

[8] H. Kali, "The Future of HR Cybersecurity: AI-Enabled Anomaly Detection in Workday Security," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, pp. 80–88, 2023.

[9] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, 2023, doi: 10.56975/tijer.v10i6.158517.

[10] M. O. Ahmad, M. A. Ahad, M. A. Alam, F. Siddiqui, and G. Casalino, "Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges," *Sensors*, vol. 21, no. 22, 2021, doi: 10.3390/s21227714.

[11] A. Mishra, "AI-Powered Cybersecurity Framework for Secure Data Transmission in IoT Network," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 3, pp. 05–13, 2025.

[12] M. M. Althobaiti, "Intelligent intrusion detection for IoT and cyber-physical systems using machine learning," *Int. J. Adv. Appl. Sci.*, vol. 12, no. 6, pp. 92–105, Jun. 2025, doi: 10.21833/ijaas.2025.06.009.

[13] S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based IoT Networks," *J. Crit. Rev.*, vol. 6, no. 07, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6:i7.13156.

[14] N. Patel, "Secure Access Service Edge(SASE): Evaluating the Impact of Convereged Network Security Architectures in Cloud Computing," *J. Emerg. Technol. Innov. Res.*, vol. 11, no. 3, 2024.

[15] S. Yaras and M. Dener, "IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm," *Electronics*, vol. 13, no. 6, p. 1053, Mar. 2024, doi: 10.3390/electronics13061053.

[16] S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection Against Cyber Attacks," *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, pp. 2102–2106, Nov. 2022, doi: 10.51219/JAIMLD/sethu-sesha-synam-neeli/461.

[17] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 01–07, 2025, doi: 10.5281/zenodo.14955016.

[18] Z. N. Hussein, D. A. Hammood, and Z. Q. Al-Abbasi, "DeepCyber-IDS: A Deep Learning Based Intrusion Detection System," in *2025 VI International Conference on Neural Networks and Neurotechnologies (NeuroNT)*, 2025, pp. 62–65. doi: 10.1109/NeuroNT66873.2025.11049980.

[19] M. A. S. P. Dayarathne, M. S. M. Jayathilaka, R. M. V. A. Bandara, V. Logeeshan, S. Kumarawadu, and C. Wanigasekara, "Mitigating Cyber Risks in Smart Cyber-Physical Power Systems Through Deep Learning and Hybrid Security Models," *IEEE Access*, vol. 13, pp. 37474–37492, 2025, doi: 10.1109/ACCESS.2025.3545637.

[20] N. Rajathi, D. S, S. A. Elavarasi, G. Saritha, and V. J. Ramya, "Adaptive Intrusion Detection in Cyber-Physical Systems Using Reinforcement Learning-Based Autoencoders," in *2024 International Conference on Integrated Intelligence and*

Communication Systems (ICIICS), 2024, pp. 1–7. doi: 10.1109/ICIICS63763.2024.10859561.

[21] J. J, P. B. M, and B. S. S, "Res2-UNeXt Combined with Federated Learning for Cyber-Attack Detection and Classification in Multi Area Smart Grid Power System," in *2024 IEEE Silchar Subsection Conference (SILCON 2024)*, 2024, pp. 1–6. doi: 10.1109/SILCON63976.2024.10910310.

[22] R. Latha and R. M. Bommi, "Hybrid CatBoost Regression model based Intrusion Detection System in IoT-Enabled Networks," in *2023 9th International Conference on Electrical Energy Systems (ICEES)*, 2023, pp. 264–269. doi: 10.1109/ICEES57979.2023.10110148.

[23] I. Ahmed, G. Jeon, and A. Ahmad, "Deep Learning-Based Intrusion Detection System for Internet of Vehicles," *IEEE Consum. Electron. Mag.*, vol. 12, no. 1, pp. 117–123, 2023, doi: 10.1109/MCE.2021.3139170.

[24] M. Abdullahi, H. Alhussian, N. Aziz, S. J. Abdulkadir, and Y. Baashar, "Deep Learning Model for Cybersecurity Attack Detection in Cyber-Physical Systems," in *2022 6th International Conference on Computing, Communication, Control and Automation, ICCUBEA 2022*, 2022. doi: 10.1109/ICCUBEA54992.2022.10010717.

[25] A. Vedant, A. Yadav, S. Sharma, O. Thite, and A. Sheikh, "Detecting Cyber Attacks in a Cyber-physical Power System: A Machine Learning Based Approach," in *2022 Global Energy Conference (GEC)*, IEEE, Oct. 2022, pp. 272–277. doi: 10.1109/GEC55014.2022.9986990.

[26] I. Mboweni, D. Ramotsoela, and A. Abu-Mahfouz, "Hydraulic Data Preprocessing for Machine Learning-Based Intrusion Detection in Cyber-Physical Systems," *Mathematics*, vol. 11, no. 8, Apr. 2023, doi: 10.3390/math11081846.

[27] V. Thangaraju, "Security Considerations in Multi-Cloud Environments with Seamless Integration: A Review of Best Practices and Emerging Threats," *Trans. Eng. Comput. Sci.*, vol. 12, no. 2, 2024.

[28] M. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, 2024, doi: 10.1186/s40537-024-00886-w.

[29] S. K. Pemmada, K. S. Naidu, and D. K. K. Reddy, "SMOTE Integrated Adaptive Boosting Framework for Network Intrusion Detection," 2024, pp. 1–25. doi: 10.1007/978-3-031-54038-7_1.

[30] M. Jouhari and M. Guizani, "Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices," *20th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2024*, pp. 1558–1563, 2024, doi: 10.1109/IWCMC61514.2024.10592352.

[31] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[32] A. Mishra, "AI-Powered Cyber Threat Intelligence System for Predicting and Preventing Cyber Attacks," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 02, pp. 873–892, 2025.

[33] N. Malali, "Cloud-Native Security and Compliance in Life and Annuities Insurance: Challenges and Best Practices," *Int. J. Interdiscip. Res. Methods*, vol. 12, no. 1, pp. 50–73, Jan. 2025, doi: 10.37745/ijirm.14/vol12n15073.

[34] K. Harahsheh, R. Al-Naimat, and C.-H. Chen, "Using Feature Selection Enhancement to Evaluate Attack Detection in the Internet of Things Environment," *Electronics*, vol. 13, no. 9, 2024, doi: 10.3390/electronics13091678.

[35] N. T. Cam and N. G. Trung, "An Intelligent Approach to Improving the Performance of Threat Detection in IoT," *IEEE Access*, vol. 11, pp. 44319–44334, 2023, doi: 10.1109/ACCESS.2023.3273160.

[36] B. M. Serinelli, A. Collen, and N. A. Nijdam, "Training Guidance with KDD Cup 1999 and NSL-KDD Data Sets of ANIDINR: Anomaly-Based Network Intrusion Detection System," *Procedia Comput. Sci.*, vol. 175, pp. 560–565, 2020, doi: 10.1016/j.procs.2020.07.080.

[37] M. M. Shirin and J. P. A. Rani, "Enhanced Intrusion Detection in Cyber Physical Systems using Graph Neural Networks," vol. 11, no. 11, pp. 3593–3598, 2025.

[38] M. Zakariah, S. A. AlQahtani, A. M. Alawwad, and A. A. Alotaibi, "Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset," *Comput. Mater. Contin.*, vol. 77, no. 3, pp. 4025–4054, 2023, doi: 10.32604/cmc.2023.043752.

