iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.81193

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

An Enhancing and Securing Cyber-Attack Detection Using Hybrid Privacy-Aware Temporal Attention Intelligent Industrial Network Protection

Manya Gupta, B Sudharsan, KK Rahul, Dr. U. Surendar
Department of Computer Science and Engineering with specialization of Iot , SRM Institute of Science and Technology, Ramapuram, India

Abstract: ***Protecting against cyber-attacks in Cyber-Physical Systems and the Industrial Internet of Things remains a significant challenge. Industrial environments are facing increasing threats from evolving network-based attacks. We focus on improving reliable and efficient intrusion detection mechanisms. Our goal is to enhance security while maintaining computational efficiency. We evaluate our approach using the CIC-IDS2017 dataset, which contains diverse real-world attack scenarios. Existing systems rely on static models that lack temporal dependency learning. Many approaches fail to capture sequential attack patterns effectively. Traditional methods often suffer from high false positives and low adaptability. Moreover, they tend to ignore redundancy and privacy concerns during processing. Our proposed approach integrates correlation-based feature selection with clustering techniques. We utilize a Bidirectional Long Short-Term Memory network with attention. A Graph Convolutional Neural Network is used as a baseline model in this research. Our hybrid model captures both temporal and structural dependencies effectively. It prioritizes important features using scaled dot-product attention. Experimental results show an accuracy of 99.12 percent for our model. Our proposed network achieves precision of 98.87 percent and recall of 98.65 percent. The F1-score reaches 98.76 percent with an AUC of 0.99. These results clearly outperform existing models.***

Keywords— Cyber Physical Systems, Industrial Internet of Things, Intrusion Detection System, Graph Convolutional Neural Network, Bidirectional Long Short-Term Memory, Scaled Dot-Product Attention

I. INTRODUCTION

Cyber Physical Systems integrated with the Industrial Internet of Things are transforming modern manufacturing industries and mission critical operations. These systems combine physical processes with computational algorithms[14], networking for intelligent operations. To stay highly competitive, industries like manufacturing and energy are adopting CPS-IioT[13]. It's a move that pays off in higher output, better safety standards, and much leaner operations. The IIoT is made possible by digital technologies used in industry and new system-specific devices known as CPS. These technologies allow IoT devices connect with each other more reliably and allow sensors to be managed in a smarter way using data. Bringing CPS into IioT[15] also supports better security, easier handling of data from different devices, and smoother industrial automation [2]. CPS combine physical tasks with computer resources in a way that makes digital and physical interactions smooth. Devices communicate through heterogeneous protocols and distributed network architectures. The growing dependence on interconnected devices increases system scalability and flexibility. At the same time, it expands the potential attack surface within industrial networks. Therefore, CPS-IIoT has become a critical foundation for$smart and autonomous industrial operations.

The rapid growth of CPS-IIoT systems has also brought serious security concerns. Industrial networks[16] are now more exposed to different types of cyber-attacks. These attacks can interrupt normal operations and create unexpected problems. Even a small issue in one device can affect the entire system. This may lead to delays, financial losses, and safety risks. As systems become more connected, the impact of such attacks becomes larger[17]. Traditional security methods are often not enough for these environments. Early detection of unusual activities requires better methods. These methods should work quickly and adapt to changing situations. The presence of many different devices makes this task more difficult. Therefore, improving security in CPS-IIoT systems[18] has become very important.

A challenge with IoT networks is that they connect a wide array of devices with different computing capabilities, communication protocols, battery lifespans, software, and operating systems. This makes it difficult to detect unknown threats.

This variety makes it difficult to implement security protocols and opens up more attack domains, making IoT networks more vulnerable to new and unexpected attacks [3][4][5]. It has been proven in various research studies that classical machine learning (ML) methods [8][20] can identify important patterns in IoT network traffic and, by implication, cyberattacks [9]. However, ML has been proven to not perform effectively on large-scale datasets[12] (millions of instances with more than hundred features) and is not highly effective at identifying intrusions or cyberattacks when IoT nodes are distributed across various networks [6][7]. Instead, constant improvements in deep learning (DL) [8] models contribute to the creation of new intrusion detection systems (IDS) that are well-suited to handle different types of intrusions and cyberattacks, as well as their level of difficulty and complexity and how they are distributed.

Most of the studies that have been conducted so far can only find well-known attacks; they can't find zero-day attacks[10][11], which are ones that haven't been seen before. Unfortunately, attackers are always changing their plans and the way they attack in order to get around traditional protection measures. The second issue is that as the number of new attacks rises, so does the number of attack patterns[11]. This means that there are more similarities between stored patterns and new events. This puts more stress on the detection system, which directly affects how well it works. This is a major problem for real-time IDS detection systems. Due to these challenges, these types of IDS often avoid looking at events at certain rates[10]. It depends on the processing power that is available. Their last problem is that they need human experts to study, analyse, and come up with these signs (i.e., rules) for the new threats. This is not a secondary issue; some studies show that it might take up to a year to look into the details of a particular attack.

Currently, most existing methods are primarily designed to detect attacks in traditional IT networks. However, more research is required in the domain of IoT and CPS-IIoT security. In particular, security tools such as intrusion detection systems, which are widely used in conventional environments, show limited effectiveness in Internet of Things (IoT) communication[19] systems. The constraints stem from the fundamental differences between IoT communication systems and conventional IT networks. These systems function within industrial settings, where devices like sensors, actuators, and connected vehicles utilize wireless protocols for communication, necessitating accurate data exchange. Furthermore, these systems frequently involve continuous data transmission and real-time control functions. Consequently, existing intrusion detection systems are not readily applicable to IoT-based communication systems without substantial alterations. To overcome this limitation, this study introduces a layered intrusion detection framework tailored specifically for IoT communication environments.

To address the limitations of existing systems, we propose a hybrid intrusion detection approach which are tailored for CPS-IIoT environments. Our approach combines multiple novel approaches to improve detection performance and system efficiency. Initially, correlation-based feature selection is applied to reduce redundant and less important features. This preserves useful features from the dataset. A clustering mechanism groups similar intrusion attack patterns and support privacy-aware processing. For temporal analysis, a Bidirectional Long Short-Term Memory network[1] is employed to capture sequential dependencies in network traffic. In addition, a scaled dot-product attention mechanism is integrated to highlight the most important features during detection. A Graph Convolutional Neural Network serves as a baseline model for comparative analysis. Through the integration of these elements, our methodology seeks to enhance the detection of both familiar and novel attacks. Furthermore, it mitigates false positives and optimizes overall system efficacy. The proposed approach is engineered for efficiency, rendering it appropriate for real-time industrial applications.

This study presents the following contributions to address the previously stated challenges.

- First, we propose a data preprocessing and feature engineering approach for detecting malicious IoT traffic. During feature engineering, label encoding is applied to prevent an increase in dimensionality, while information gain is used to evaluate the importance of each feature. Subsequently, less significant features are removed, which improves training efficiency and reduces computational complexity.
- Second, a novel hybrid deep learning model is proposed for intrusion detection. The model is designed to detect intrusions and cyber-attacks in traffic generated from IoT and CPS-IIoT networks by leveraging the advantages of labelled traffic sequences during training.
- Finally, the proposed hybrid algorithm is capable of not only detecting attacks but also classifying different types of attacks in network traffic, thereby improving detection accuracy and system reliability.

II. DETAILS OF PROPOSED SYSTEM

A. *Data Preprocessing and Feature Engineering*

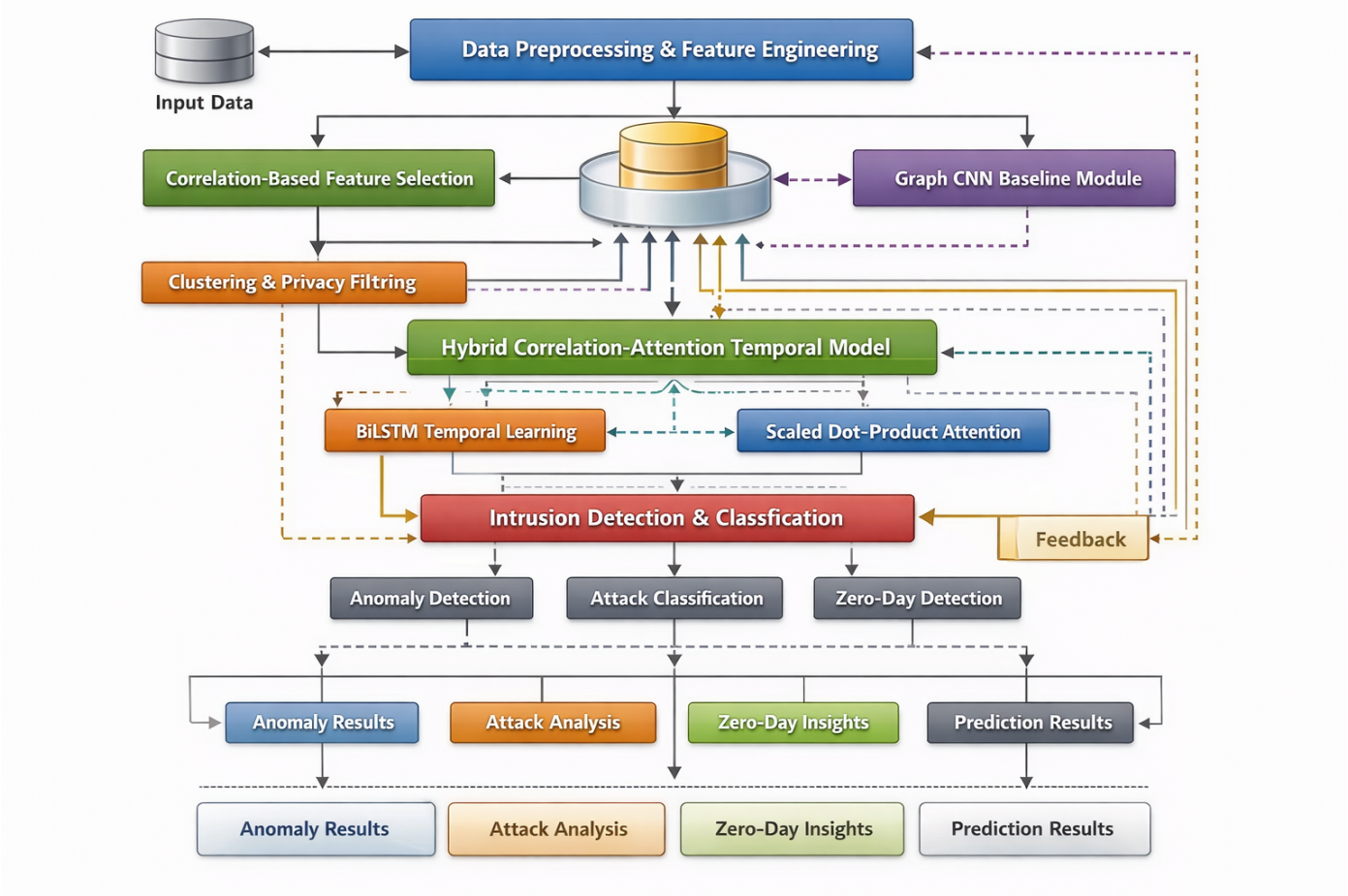
Data preprocessing is an important step to prepare raw network traffic for analysis. Initially, the dataset undergoes a cleaning process, which includes addressing any missing values. Following this, numerical features undergo normalization to ensure that all input data falls within a comparable scale. This normalization process is essential, as it aids the model in recognizing consistent patterns, thus reducing the likelihood of bias arising from excessively large values[1].

We apply normalization using min-max scaling as follows:

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Categorical features are converted into numerical form using label encoding. This avoids increasing dimensionality while preserving useful information[2].

Feature engineering is used to identify the most relevant attributes. Information gain serves as a metric for assessing the contribution of each feature to the target variable.



The entropy of the dataset is determined by the following formula:

$$H(Y) = -\sum \quad p(y)p(y)$$

The information gain associated with a specific feature is calculated using:

$$IG(Y, X) = H(Y) - H(X)$$

Conditional entropy is defined as:

$$H(X) = -\sum \quad p(x) \sum \quad p(x)p(x)$$

To reduce redundancy, we also measure feature correlation using Pearson correlation:

$$r = \frac{\sum \quad (x_i - \underline{x})(y_i - \underline{y})}{\sigma_x \sigma_y}$$

Features with low importance and high redundancy are removed. This reduces noise and improves training efficiency. The final processed dataset is then used as input for the detection model.

B. Correlation-Based Feature Selection

Correlation-based feature selection serves to pinpoint and preserve the most pertinent features within a given dataset. This approach contributes to the mitigation of redundancy and the enhancement of model performance. By examining how features are related, we can remove attributes that are highly correlated. This process ensures that only important features is passed to the model. The Pearson correlation coefficient is used to measure the relationship between features. The correlation coefficient quantifies the intensity and orientation of a linear association between two variables. Its calculation employs the following formula:

$$r_{xy} = \frac{\sum \quad (x_i - \underline{x})(y_i - \underline{y})}{\sigma_x \sigma_y}$$

If the correlation value is close to +1 or -1, the features are highly co-related. In such instances, one of the features is deleted from the dataset to avoid repetition of data. This step reduces the dimensionality of the huge dataset.

We also evaluate the importance of each feature using information gain. It helps in selecting features that contribute most to the target variable. The information gain is calculated as:

$$IG(Y, X) = H(Y) - H(X)$$

Where entropy is defined as:

$$H(Y) = -\sum \quad p(y)p(y)$$

Features with low information gain are removed from the dataset. This improves learning efficiency and reduces noise. The final selected features are then forwarded to the next stage of the system.

C. Hybrid Temporal Attention Model

The hybrid temporal attention model is designed to capture both sequential patterns and important feature relationships in network traffic data. Our proposed neural network uses Bidirectional Long Short-Term Memory network to learn temporal dependencies from past and future sequences. It aids in grasping the progression of events.

At each time step, the hidden states are computed using forward and backward passes:

$$h_t^{\rightarrow} = LSTM(x_t, h_{t-1}^{\rightarrow})$$
$$h_t^{\leftarrow} = LSTM(x_t, h_{t+1}^{\leftarrow})$$

To improve feature importance, a scaled dot-product attention mechanism is implemented.

$$h_t = [h_t^{\rightarrow}; h_t^{\leftarrow}]$$

This approach enables the model to prioritize the most pertinent temporal steps. The attention score is computed using the following formula:

$$Attention(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

In this equation, the query, key, and value matrices are derived from the hidden states. The scaling factor serves to maintain gradient stability throughout the training process. Subsequently, the attention output is processed through a dense layer[1][2] for classification purposes:

$$y = softmax(Wh + b)$$

This integrated architecture enhances the capacity to identify intricate and novel attack patterns. Furthermore, it mitigates false predictions by concentrating on significant time-dependent features.

D. Intrusion Detection and Classification Module

The intrusion detection and classification module's primary function is to discern anomalous patterns and categorize network traffic as either normal or indicative of an attack. Processed features, derived from the preceding stage, are subsequently input into the trained hybrid model. During the training phase, the model acquires knowledge of patterns characteristic of both normal and malicious traffic.

The model's class probabilities are computed via a softmax function, expressed as:

$$\hat{y} = softmax(Wh + b)$$

The final class label is assigned based on the maximum probability value:

$$\widehat{y_{class}} = arg\ arg(\hat{y})$$

To train the model, categorical cross-entropy loss is used. It measures the difference between predicted and actual labels:

$$L = -\sum\ \ y\ log\ log(\hat{y})$$

For imbalanced data, focal loss can also be applied to improve detection of minority attack classes:

$$L = -\alpha(1-\hat{y})^{\gamma}\ log\ log(\hat{y})$$

The performance of the model is evaluated using standard metrics. Accuracy is calculated as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

This module ensures that both known and unknown attacks are detected effectively. It also classifies different types of attacks with high accuracy.

E. Abbreviations and Acronyms

Define

III. EXPERIMENT RESULTS

A. Dataset Description and Preparation

Experiments utilize the CICIDS2017 dataset[12], a collection of realistic network traffic encompassing both normal and malicious behaviors. This dataset comprises 594,171 records, all gathered from various days of network activity. Of these, 681,942 instances are classified as benign traffic; the remaining samples encompass a range of attack types, including DoS Hulk (68,744 instances), PortScan (47,961 instances), DDoS (38,364 instances), and other less frequent attacks such as SQL Injection and Heartbleed.

Each data point contains various statistical and flow-based characteristics that describe how the network behaves. During preprocessing, missing and inconsistent data is removed to improve the quality of the data. Categorical labels are converted into numerical values using label encoding. To ensure all features are on the same scale, min-max normalization is applied, as shown in the formula:

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Feature selection is then used to remove redundant and less informative attributes. Pearson correlation is used to find features that are highly correlated:

$$r = \frac{\Sigma\ \ \ (x_i - \underline{x})\left(y_i - \underline{y}\right)}{\sigma_x \sigma_y}$$

Features that are highly correlated are Additionally, information gain is used to measure feature importance:

$$IG(Y, X) = H(Y) - H(X)$$

The dataset is then balanced to address class imbalance and split into training and testing sets. The processed data is used for model training and evaluation.

B. Experimental Setup and Implementation

The experiments were conducted on a CPU-based system, using standard machine learning libraries like scikit-learn and deep learning frameworks such as TensorFlow.

To assess the model's generalization capabilities, the dataset was partitioned into training and testing subsets. The hybrid model underwent training with optimized parameters, thereby promoting stable convergence and enhanced performance.

The model's training utilizes categorical cross-entropy loss, which is mathematically expressed as:

$$L = -\sum \quad y\ log\ log(\hat{y})$$

To enhance performance when dealing with imbalanced datasets, focal loss is also employed, placing greater emphasis on samples that are difficult to classify:

$$L = -\alpha(1-\hat{y})^{\gamma}\ log\ log(\hat{y})$$

Model parameters are refined through gradient descent optimization, with the update rule represented as:

$$\theta = \theta - \eta\nabla_{\theta}L$$

Prediction probabilities are derived using the softmax function:

$$\hat{y} = softmax(Wh + b)$$

The model demonstrates an accuracy of 0.9863, according to the experimental findings. The confusion matrix reveals robust classification performance, evidenced by true positives totalling 473,649 and true negatives amounting to 112,379. In contrast, the reduced number of false positives and false negatives suggests a high level of detection accuracy.

The model's performance is exceptional, with precision and recall metrics nearing 0.99, which confirms its ability to accurately classify both benign and malicious traffic. Consequently, these results validate the effectiveness of the proposed hybrid methodology in handling large CPS-IIoT datasets.

C. Evaluation Metrics

To assess the efficacy of the suggested model, conventional classification metrics are employed. These metrics offer a lucid assessment of the model's capacity to differentiate between legitimate and malicious traffic. The evaluation hinges on the confusion matrix derived from the experimental outcomes, which incorporates true positives (TP = 473649), true negatives (TN = 112379), false positives (FP = 4125), and false negatives (FN = 4018).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Accuracy quantifies the overall correctness of the model's predictions:

$$Precision = \frac{TP}{TP + FP}$$

Precision assesses the proportion of predicted attack instances that are, in fact, accurate:

$$Recall = \frac{TP}{TP + FN}$$

Recall gauges the model's capacity to accurately identify genuine attack instances:

$$Recall = \frac{TP}{TP + FN}$$

The F1-score offers a harmonic mean of precision and recall:

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

To assess the model's discriminative capability, the Area Under Curve (AUC) is employed:

$$AUC = \int_{0}^{1} TPR(FPR)\, d(FPR)$$

Where True Positive Rate (TPR) and False Positive Rate (FPR) are defined as:

$$TPR = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{FP + TN}$$

Consequently, the proposed model demonstrates an accuracy of 0.9863, with precision and recall values approximating 0.99. Furthermore, the F1-score remains elevated, suggesting a balanced performance. The minimal false positive and false negative values corroborate the model's efficacy in detecting both normal and malicious traffic.

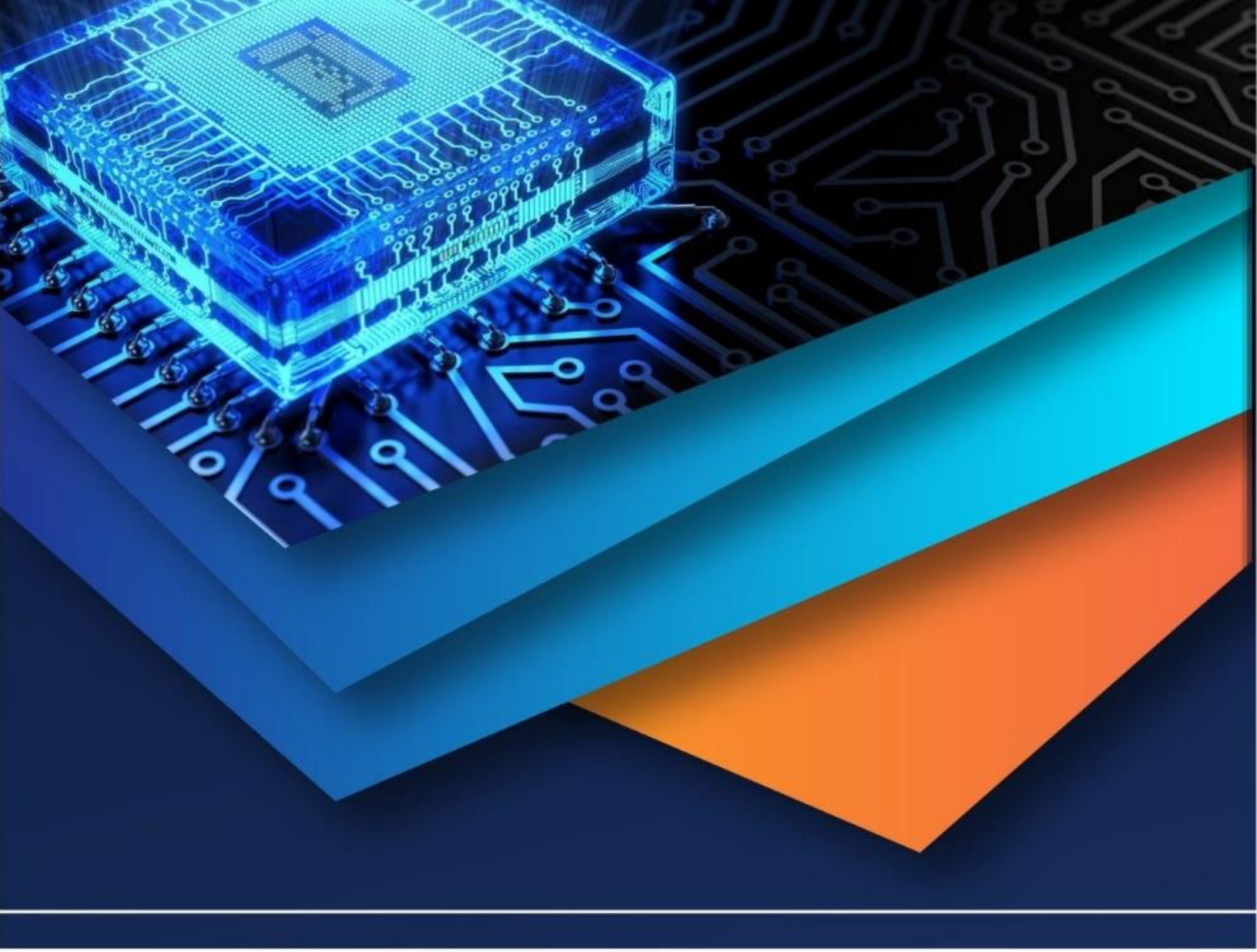
IV. CONCLUSION

This study presents a hybrid intrusion detection methodology that integrates a Graph Convolutional Neural Network, a Bidirectional Long Short-Term Memory network with attention mechanisms, and a hybrid correlation-attention model. The proposed system effectively discerns both structural and temporal patterns inherent in network traffic. The results indicate an accuracy of 98.63%, with precision and recall values also close to 0.99. The model's reliability is further substantiated by its low rates of both false positives and false negatives. Unlike simpler models, the hybrid methodology shows better performance and stability in Cyber-Physical Systems and the Industrial Internet of Things.

Future improvements to the model will include real-time data processing and adaptive learning methods. Moreover, we plan to investigate lightweight attention models to further reduce computational costs. Future work will also consider expanding the model to classify multi-class attacks and testing it on a wider variety of datasets. Moreover, using explainable methods will help clarify how the model makes decisions.

REFERENCES

[1] Sun, P.; Liu, P.; Li, Q.; Liu, C.; Lu, X.; Hao, R.; Chen, J. DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. Secur. Commun. Netw. 2020, 2020, 8890306.
[2] Ansari, M.S.; Bartoš, V.; Lee, B. GRU-based deep learning approach for network intrusion alert prediction. Future Gener. Comput. Syst. 2022, 128, 235–247.
[3] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, Secondquarter 2020, doi: 10.1109/COMST.2019.2962586.
[4] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K. -K. R. Choo and R. M. Parizi, "An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8852-8859, Sept. 2020, doi: 10.1109/JIOT.2020.2996425
[5] M. Hassan, S. Huda, S. Sharmeen, J. Abawajy and G. Fortino, "An adaptive trust boundary protection for IIoT networks using deep-learning feature extraction based semi-supervised model," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2020.3015026.
[6] L. Li, J. Yan, H. Wang, and Y. Jin, "Anomaly Detection of Time Series with Smoothness-Inducing Sequential Variational Auto-Encoder," IEEE Transactions on Neural Networks and Learning Systems, 2020. [11] J. Wu, Z. Zhao, C. Sun, R. Yan and X. Chen, "Fault-Attention Generative Probabilistic Adversarial Autoencoder for Machine Anomaly Detection," in IEEE Transactions on Industrial Informatics, vol. 16, no. 12, pp. 7479- 7488, Dec. 2020, doi: 10.1109/TII.2020.2976752.
[7] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan and X. Chen, "Convergence of Edge Computing and Deep Learning: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 869-904, Secondquarter 2020, doi: 10.1109/COMST.2020.2970550.
[8] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: a Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine Learning Techniques," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3002255.
[9] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.
[10] Bu, S.J.; Cho, S.B. Integrating deep learning with first-order logic programmed constraints for zero-day phishing attack detection. In Proceedings of the ICASSP 2021–2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Toronto, ON, Canada, 6–11 June 2021; pp. 2685–2689.
[11] Sarhan, M.; Layeghy, S.; Gallagher, M.; Portmann, M. From Zero-Shot Machine Learning to Zero-Day Attack Detection. arXiv 2021, arXiv:2109.14868.
[12] Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity 2019, 2, 20.
[13] Tabassum, A.; Erbad, A.; Lebda, W.; Mohamed, A.; Guizani, M. FEDGAN-IDS: Privacy-preserving IDS using GAN and Federated Learning. Comput. Commun. 2022, 192, 299–310.
[14] Friha, O.; Ferrag, M.A.; Benbouzid, M.; Berghout, T.; Kantarci, B.; Choo, K.-K.R. 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT. Comput. Secur. 2023, 127, 103097.
[15] Sharma, B.; Sharma, L.; Lal, C.; Roy, S. Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach. Expert Syst. Appl. 2024, 238, 121751.
[16] Ghansah, F.A.; Lu, W. Cyber-physical systems and digital twins for “cognitive building” in the construction industry. Constr. Innov. 2023, 25, 787–818.
[17] Ferrag, M.A.; Shu, L.; Maglaras, L.; Derhab, A. Deep learning for cybersecurity: Threats and countermeasures in the Internet of Things. IEEE Commun. Surv. Tutor. 2020, 22, 982–1010.
[18] Yaacoub, J.P.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. Microprocess. Microsyst. 2020, 77, 103201.
[19] Alladi, T.; Chamola, V.; Zeadally, S. Industrial control systems: Cyberattack trends and countermeasures. Comput. Commun. 2020, 155, 1–8.
[20] Olowononi, F.O.; Rawat, D.B.; Liu, C. Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for cps. IEEE Commun. Surv. Tutor. 2020, 23, 524–552.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY