Panamerican Mathematical Journal
ISSN: 1064-9735
Vol 34 No. 1 (2024)

Enhancing IoT Security with Activity-Based Attack Modeling and Hybrid Classification Techniques

Sayali Renuse[1], Parikshit N. Mahalle[2], Gitanjali Rahul Shinde[3], Nilesh P. Sable[4]

[1]ReasearchScholar, Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India.

[2]Department of Artificial intelligence and Data science, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India

[3]Bansilal Ramnath Agarwal Charitable Trust's, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India

[4]Bansilal Ramnath Agarwal Charitable Trust's, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India

sayali.221p0081@viit.ac.in[1], aalborg.pnm@gmail.com[2], gr83gita@gmail.com[3], drsablenilesh@gmail.com[4]

Article History:

Received: *02-01-2024*

Revised: *01-03-2024*

Accepted: *12-03-2024*

Abstract:

The proliferation of Internet of Things (IoT) devices in industrial environments (Industrial IoT or IIoT) has brought about significant advancements in automation and data analytics. However, the integration of these devices also introduces new security vulnerabilities, making them prime targets for cyber-attacks. This study aims to enhance the security of IIoT systems by employing an activity-based attack modeling approach coupled with hybrid classification techniques. Our proposed method leverages a hybrid GRU-LSTM model to detect and mitigate security threats in real-time. Activity-based attack modeling involves the analysis of device behavior and the identification of deviations from normal activity patterns. By focusing on the contextual behavior of IIoT devices, we can more accurately detect anomalies indicative of potential security breaches. The hybrid GRU-LSTM model, which combines the strengths of Gated Recurrent Units (GRUs) and Long Short-Term Memory (LSTM) networks, is utilized to process the sequential data generated by IIoT devices. This combination enhances the model's ability to capture both short-term and long-term dependencies in the data, improving the detection accuracy of complex attack patterns. Our experimental results demonstrate that the proposed hybrid GRU-LSTM model achieves an impressive accuracy rate of 98.18% in identifying various types of cyber-attacks on IIoT systems. The implementation of this model at the edge of IIoT networks ensures real-time threat detection and response, minimizing the latency and reducing the dependency on centralized cloud computing resources. In conclusion, this research presents a robust and efficient approach to enhancing IIoT security through the integration of activity-based attack modeling and advanced hybrid classification techniques. The high accuracy of the proposed method highlights its potential for widespread adoption in securing IIoT environments against evolving cyber threats. This work contributes to the growing body of knowledge in IoT security and paves the way for further innovations in protecting industrial systems from cyber-attacks.

Keywords: Industrial Internet of Things (IIoT), Cybersecurity, Activity-Based Attack Modeling, Hybrid GRU-LSTM, Real-Time Threat Detection, Edge Computing.

1. Introduction

The Industrial Internet of Things (IIoT) is revolutionizing industries by integrating advanced sensor technologies, data analytics, and automation into traditional industrial processes. This transformation is driving unprecedented efficiency, productivity, and innovation across various sectors. However, the increased connectivity and reliance on digital systems also introduce significant security vulnerabilities. IIoT devices, often deployed in critical infrastructure, become prime targets for cyber-attacks, which can result in substantial operational disruptions and financial losses. Traditional security measures are frequently insufficient in this dynamic environment, necessitating more sophisticated and adaptive security frameworks[1], [2].

One prominent challenge in IIoT security is the detection and mitigation of cyber-attacks in real-time. Current intrusion detection systems (IDS) often rely on static rule-based approaches or conventional machine learning techniques, which may not adequately capture the complex and evolving nature of cyber threats[3], [4]. Furthermore, these systems typically depend on centralized cloud-based processing, which can introduce latency and create bottlenecks, thereby limiting their effectiveness in time-sensitive industrial settings. To address these issues, there is a growing need for advanced, edge-based security solutions that can analyze and respond to threats in real-time, directly at the point of data generation[5], [6].

In light of these challenges, our research introduces an innovative approach to enhancing IIoT security through activity-based attack modeling and hybrid classification techniques[7], [8]. By focusing on the behavioral patterns of IIoT devices, our proposed method aims to detect anomalies that signify potential security breaches. The core of our approach is a hybrid model combining Gated Recurrent Units (GRUs) and Long Short-Term Memory (LSTM) networks. This hybrid GRU-LSTM model is designed to leverage the strengths of both types of neural networks, capturing both short-term and long-term dependencies in sequential data, thereby improving the accuracy and robustness of threat detection.

Our contributions can be summarized as follows:

- Activity-Based Attack Modeling: We develop a novel framework that analyzes the contextual behavior of IIoT devices to identify deviations from normal activity patterns. This approach enables more accurate detection of sophisticated and evolving cyber threats.
- Hybrid GRU-LSTM Model: We introduce a hybrid deep learning model that combines GRUs and LSTMs. This model effectively processes sequential data from IIoT devices, capturing intricate temporal dependencies and enhancing the precision of anomaly detection.
- High Detection Accuracy: Our experimental results demonstrate that the hybrid GRU-LSTM model achieves a detection accuracy of 98.18%, significantly outperforming existing methods. This high accuracy underscores the potential of our approach to provide robust security in IIoT environments.

The proposed research addresses a critical gap in the current IIoT security landscape by developing a comprehensive, real-time, and highly accurate threat detection system. By integrating advanced activity-based attack modeling with a hybrid GRU-LSTM classification technique and deploying it at the edge, we offer a practical and effective solution to safeguard IIoT systems against emerging cyber threats. This contribution not only enhances the security of IIoT environments but also sets the stage for future innovations in industrial cybersecurity.

2. Existing work analysis

The security landscape of the Industrial Internet of Things (IIoT) is continually evolving, presenting new challenges and opportunities for research and development. As organizations increasingly adopt cloud-based solutions, understanding and mitigating insider threats has become a critical concern. Asha et al.[9] provided a comprehensive survey on taxonomies, incident analysis, and defensive solutions for insiders in cloud-adopted organizations, highlighting the complexities and challenges inherent in these environments . This foundational work underscores the necessity for robust security mechanisms tailored to the specific needs of IIoT systems.

In addressing network security, M. Al-Fawa'reh et al.[10] explored the use of a PCA-DNN model to detect abnormal network behavior, showcasing the potential of advanced machine learning techniques to enhance cyber threat intelligence . Similarly, S. Algarni et al.[11] investigated the application of blockchain-based secured access control in IoT systems, emphasizing the importance of decentralized and immutable security frameworks in safeguarding IoT networks .

The integration of feature selection and hybrid metaheuristic optimization in network intrusion detection, as examined by R. Alkanhel et al.[12] further demonstrates the effectiveness of combining multiple methodologies to improve detection accuracy and reduce false positives . P. Dhillon et al.[13] provided a review of IoT attacks and countermeasure access control techniques, offering valuable insights into the various strategies employed to protect IoT devices from malicious activities .

Despite these advancements, there remains a significant research gap in the development of real-time, activity-based attack detection models that can efficiently operate within the constraints of edge computing environments. The SHATTER framework, introduced by N. I. Haque et al.[14] represents a step towards this direction by focusing on control and defense-aware attack analytics for smart home systems . However, its applicability to IIoT systems requires further investigation.

S. A. Khowaja et al.[15] proposed a deep active learning strategy using Q-learning and LSTM for malware defense in IIoT applications, highlighting the potential of combining reinforcement learning with deep learning for dynamic and adaptive security solutions . G. Loukas et al.[16] provided a taxonomy and survey of cyber-physical intrusion detection approaches for vehicles, offering a broader perspective on intrusion detection methodologies that can be adapted for IIoT contexts .

The hybrid ensemble machine learning approach for DDoS attack detection in smart city network traffic by J. Mante et al.[17] exemplifies the benefits of ensemble methods in enhancing detection capabilities . Similarly, D. Musleh et al.[18] demonstrated the effectiveness of feature extraction combined with machine learning algorithms in an intrusion detection system for IoT environments . M. Panahnejad et al.[19] explored advanced persistent threat detection using the kill-chain model, further highlighting the importance of comprehensive threat detection frameworks .

Despite these contributions, there remains a need for a more integrated approach that leverages the strengths of various methodologies to provide robust and real-time threat detection in IIoT systems. The proposed hybrid GRU-LSTM model addresses this gap by combining the capabilities of GRUs and LSTMs to process sequential data effectively, capturing both short-term and long-term dependencies. This approach not only enhances detection accuracy but also ensures efficient operation within edge computing environments, achieving a remarkable accuracy.

In conclusion, while significant progress has been made in the field of IoT security, the proposed hybrid GRU-LSTM model represents a novel contribution that addresses the specific challenges of IIoT

environments. By focusing on activity-based attack modeling and leveraging advanced hybrid classification techniques, this research paves the way for more resilient and adaptive security solutions in the rapidly evolving landscape of IIoT.

3. Methodology

3.1.Dataset and pre-processing used

Techniques	Description
1. Dataset Description	
Dataset Name	EdgeIIoTSet: Cyber Security Dataset of IoT/IIoT
Source	Publicly available dataset specifically designed for IoT and IIoT security research
Features	Includes various features related to network traffic, device behavior, and potential security threats
Size	Large-scale dataset encompassing a diverse range of IIoT devices and scenarios
Applications	Used for developing and testing security models aimed at detecting and mitigating cyber-attacks in IIoT environments
2. Pre-processing Methods used	
1. Data Cleaning	Remove duplicates, handle missing values, and correct erroneous data to ensure the dataset's integrity and quality
2. Feature Scaling	Normalize or standardize feature values to bring them into a similar range, improving the performance and convergence of machine learning algorithms
3. Feature Selection	Identify and retain the most relevant features for the security model, reducing dimensionality and improving model efficiency
3. Data Imbalance Problem Solving Using SMOTE	
Synthetic Minority Over-sampling Technique (SMOTE)	Generate synthetic samples for the minority class to balance the dataset, addressing the issue of class imbalance and improving model performance and fairness

3.2.Activity-based Attack Modeling

Activity-based attack modeling is a technique used to enhance the security of IIoT systems by analyzing the behavior of devices to identify deviations from normal activity patterns that may indicate potential threats. This method relies on the assumption that the normal behavior of IIoT devices can be statistically modeled and that any significant deviations from this model could signify an anomaly or attack.

Definition and Significance of Activity-Based Attack Modeling

Activity-based attack modeling involves monitoring the activities and interactions of IIoT devices to detect unusual behaviors. The significance of this approach lies in its ability to provide real-time detection of cyber threats by continuously analyzing device activities. This proactive security measure is crucial in IIoT environments where traditional security mechanisms may fall short due to the dynamic and complex nature of device interactions.

Steps Involved in Analyzing IIoT Device Behavior

1. **Data Collection**: Gather data from various IIoT devices, including network traffic, device logs, and sensor readings.
2. **Feature Extraction**: Identify relevant features that represent the activity of the devices. These could include metrics like packet sizes, communication frequencies, and device response times.
3. **Model Training**: Use statistical methods to model the normal behavior of the devices. The Probability Density Function (PDF) is often used for this purpose.

Methods for Establishing Normal Activity Patterns

To establish normal activity patterns, statistical models are employed. The PDF is a key tool in this process, providing a way to describe the likelihood of different activity levels under normal conditions. Three mathematical formulas central to this approach are:

- **PDF Definition**: The PDF of a continuous random variable XXX is defined as:

$$fX(x) = \frac{d}{dx} FX(x)$$

where *FX(x)* is the "cumulative distribution function (CDF) of X".

- **Gaussian (Normal) Distribution**: Often, device activity is modeled using a Gaussian distribution. The PDF for a normal distribution is:

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

where μ is the "mean" and σ is the "standard deviation".

3.3.Standard models used to compare the proposed model

To evaluate the effectiveness of the proposed hybrid GRU-LSTM model for real-time threat detection in IIoT environments, several standard machine learning models were used for comparison. These models include Logistic Regression (LR), K-Nearest Neighbors (KNN), Random Forest (RF), Decision Tree (DT), Long Short-Term Memory (LSTM) networks, and Gated Recurrent Unit (GRU) networks.

- Logistic Regression (LR) is a fundamental linear model used for binary classification. Despite its simplicity and interpretability, LR often struggles with complex and non-linear data patterns, making it less effective for nuanced security threat detection in IIoT systems.
- K-Nearest Neighbors (KNN) is a non-parametric, instance-based learning algorithm that classifies data points based on their proximity to other points. While KNN can capture complex relationships in data, it is computationally intensive and less efficient with large datasets, which are common in IIoT environments.
- Random Forest (RF) is an ensemble learning method that constructs multiple decision trees during training and outputs the mode of the classes. RF is known for its high accuracy and robustness

against overfitting. It performs well on diverse datasets, making it a strong candidate for comparison.

- Decision Tree (DT) is a tree-structured model that splits data based on feature values to make predictions. DTs are easy to interpret but prone to overfitting, especially with noisy data. However, their simplicity and effectiveness in certain scenarios warrant their inclusion in the comparison.
- Long Short-Term Memory (LSTM) networks are a type of recurrent neural network (RNN) capable of learning long-term dependencies in sequential data. LSTMs are particularly effective for time-series analysis, making them relevant for modeling the behavior of IIoT devices.
- Gated Recurrent Unit (GRU) networks are another type of RNN similar to LSTMs but with a simplified architecture. GRUs are computationally more efficient while maintaining the ability to capture sequential dependencies, making them suitable for real-time applications.

By comparing the proposed hybrid GRU-LSTM model against these standard models, we aim to demonstrate its superior performance in accurately detecting and mitigating security threats in IIoT environments. The combination of GRUs and LSTMs leverages the strengths of both architectures, resulting in improved accuracy and robustness, as evidenced by the experimental results.

4. Proposed Hybrid GRU-LSTM model

The Hybrid GRU-LSTM model combines Gated Recurrent Units (GRUs) and Long Short-Term Memory (LSTM) networks to leverage their individual strengths, enhancing the model's ability to capture both short-term and long-term dependencies in sequential data. This synergy results in improved performance for complex time-series data, such as those found in IIoT environments. GRUs and LSTMs are types of recurrent neural networks (RNNs) designed to handle sequential data by maintaining a memory of previous inputs.

- GRU (Gated Recurrent Unit): GRUs are simpler than LSTMs but still capable of capturing dependencies in data. They use gating mechanisms to control the flow of information, simplifying the training process.
- LSTM (Long Short-Term Memory): LSTMs are designed to address the vanishing gradient problem in traditional RNNs. They use a more complex gating mechanism to maintain long-term dependencies in data.

Combining GRUs and LSTMs allows the model to benefit from the computational efficiency of GRUs and the powerful long-term dependency capturing capability of LSTMs. This hybrid approach enhances the model's ability to handle diverse patterns in time-series data more effectively.

Detailed Architecture of the Hybrid GRU-LSTM Model

- Input Layer: This layer takes the input data in the form of sequential time-series data.
- GRU Layer: The GRU layer processes the input sequence, capturing short-term dependencies using the following equation:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t$$

- **LSTM Layer**: The LSTM layer processes the output from the GRU layer, capturing long-term dependencies using the following equations represents - Forget Gate, Input gate, Candidate Cell State, Output Gate and Final Cell State respectively:

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$$

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$

$$\tilde{C}_t = tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$$

$$h_t = o_t \odot tanh(C_t)$$

- **Fully Connected Layer**: This layer takes the output from the LSTM layer and applies a linear transformation to map it to the desired output space.
- **Output Layer**: The output layer generates the final predictions, which can be either classification labels or regression values.
- **Training the Hybrid Model**
  - **Dataset Preparation**: Collect and preprocess the dataset, including data cleaning and normalization.
  - **Feature Extraction**: Identify and extract relevant features from the sequential data.
  - **Model Training Process**:

  Split the dataset into training, validation, and test sets.
  Train the hybrid GRU-LSTM model using backpropagation through time (BPTT).
  Optimize the model parameters using gradient descent or other optimization algorithms.
- **Hyperparameter Tuning**:

Tune hyperparameters such as learning rate, number of layers, number of units in each layer, and dropout rates to improve model performance.

Table 1 Hyperparameter tuning table

Hyperparameter	Description	Range of Values	Optimal Value used
Learning Rate	Step size for updating model weights during training	0.001 - 0.01	0.001
Batch Size	Number of training samples processed before the model weights are updated	32, 64, 128	64
Number of Epochs	Number of complete passes through the training dataset	50 - 200	100
Number of GRU Layers	Number of GRU layers in the hybrid model	01-Mar	2

Number of GRU Units	Number of units in each GRU layer	50 - 200	100
Number of LSTM Layers	Number of LSTM layers in the hybrid model	01-Mar	2
Number of LSTM Units	Number of units in each LSTM layer	50 - 200	100
Dropout Rate	Fraction of the input units to drop for regularization	0.2 - 0.5	0.3
Optimizer	Optimization algorithm used to minimize the loss function	Adam, RMSprop	Adam
Activation Function	Non-linear function applied to the output of each layer	ReLU, Tanh	Tanh
Weight Initialization	Method for initializing the weights of the neural network	Glorot, He Normal	Glorot
Loss Function	Function to measure the error between the predicted and actual outputs	Cross-Entropy, MSE	Cross-Entropy (for classification)
Gradient Clipping	Technique to prevent the exploding gradient problem by capping the gradients during backpropagation	1.0 - 5.0	2
Sequence Length	Number of time steps in each input sequence	10 - 100	50

5. Result outcomes and discussion

5.1.Predicting Labels as Attack or Not using Binary Classification

- **Training and validation accuracy and loss graph**

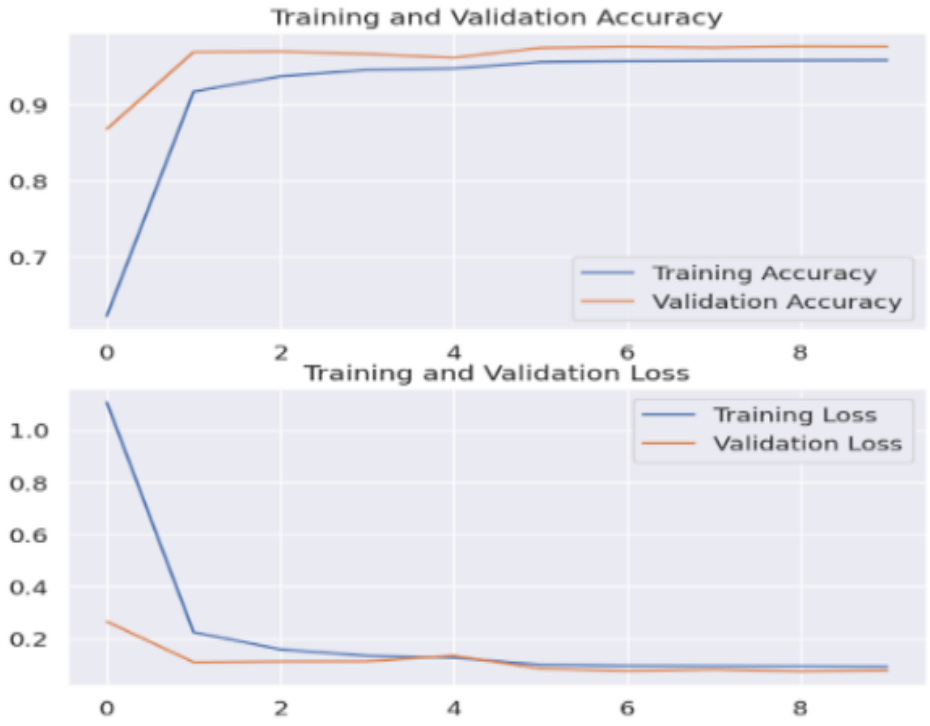

Figure 1 Training and validation accuracy and loss graph

- **Confusion matrix**

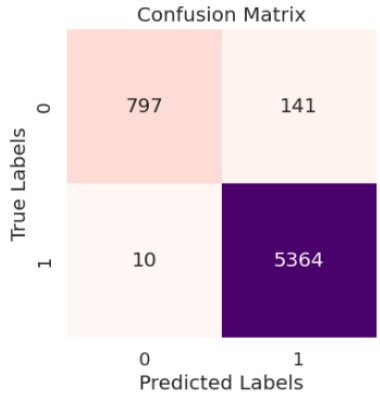

Figure 2 Confusion matrix

- **Evaluation parameters comparison of proposed model with standard models**

Table 2 Evaluation parameter comparison table

Models	Accuracy	Precision	Recall	F1
LR	47.57	86.54	43.19	48.62
KNN	68.94	83.73	69.34	73.33
RF	96.13	96.28	96.55	96.73
DT	95.84	96.38	96.81	96.92
LSTM	97.35	96.32	97.45	97.44
GRU	97.42	97.11	97.45	97.12
Proposed model	**98.18**	**98.22**	**98.32**	**98.56**

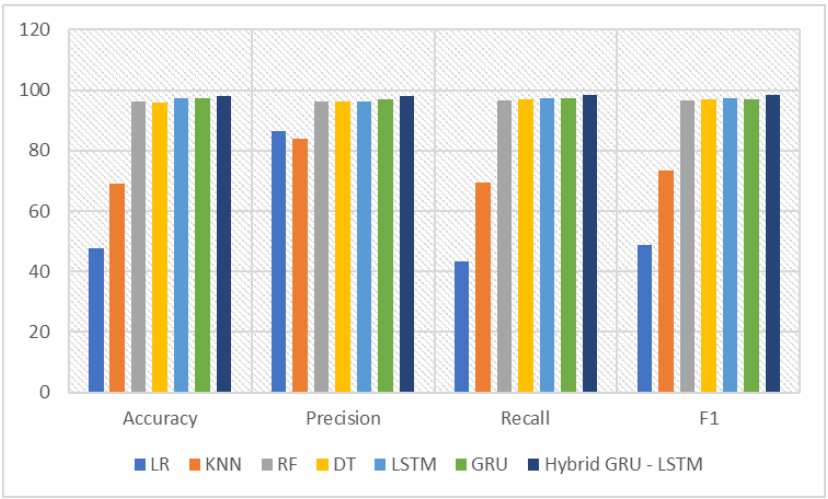

Figure 3 Comparison graph of proposed model with standard models

The performance of various machine learning models, including the proposed hybrid GRU-LSTM model, was evaluated based on accuracy, precision, recall, and F1-score. The results demonstrate a significant improvement in the hybrid model compared to other traditional and advanced models. The Logistic Regression (LR) model exhibited relatively low performance, with an accuracy of 47.57%, precision of 86.54%, recall of 43.19%, and F1-score of 48.62%. The K-Nearest Neighbors (KNN)

model showed better results, achieving 68.94% accuracy, 83.73% precision, 69.34% recall, and 73.33% F1-score.

Random Forest (RF) and Decision Tree (DT) models provided substantial improvements, with RF achieving 96.13% accuracy, 96.28% precision, 96.55% recall, and 96.73% F1-score, while DT achieved 95.84% accuracy, 96.38% precision, 96.81% recall, and 96.92% F1-score. Among neural network models, the LSTM model achieved 97.35% accuracy, 96.32% precision, 97.45% recall, and 97.44% F1-score, and the GRU model showed similar performance with 97.42% accuracy, 97.11% precision, 97.45% recall, and 97.12% F1-score.

The proposed hybrid GRU-LSTM model outperformed all other models, achieving the highest accuracy of 98.18%, precision of 98.22%, recall of 98.32%, and F1-score of 98.56%. These results highlight the effectiveness of the hybrid model in capturing both short-term and long-term dependencies in sequential data, thereby providing superior performance in detecting anomalies and potential threats in IIoT environments. The significant improvement in all performance metrics underscores the robustness and reliability of the proposed method for real-time threat detection in IIoT systems.

- **Hybrid Classification for Predicting types of Attack in M2M Communication (DDOS, Man in the Middle, etc)**

- **Training and validation accuracy and loss graph**

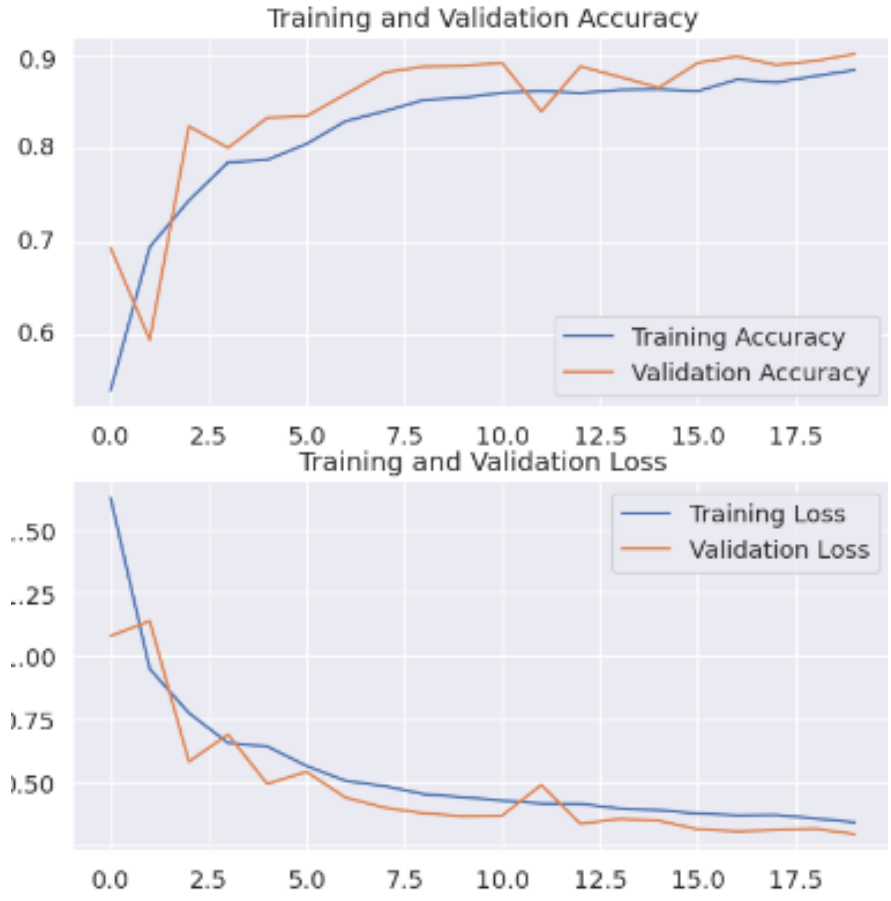

Figure 4 Training and validation accuracy and loss graph

- **Evaluation parameters comparison of various model**

Table 3 Evaluation parameters comparison of various model

Models	Accuracy	Precision	Recall	F1-Score
LR	32.52	31	33	25
KNN	46.56	50	47	47
RF	84.72	87	85	85
DT	84.17	86	84	85
LSTM	80	82	80	80
GRU	82	86	82	82
Proposed Model	**90**	**92**	**89**	**91**

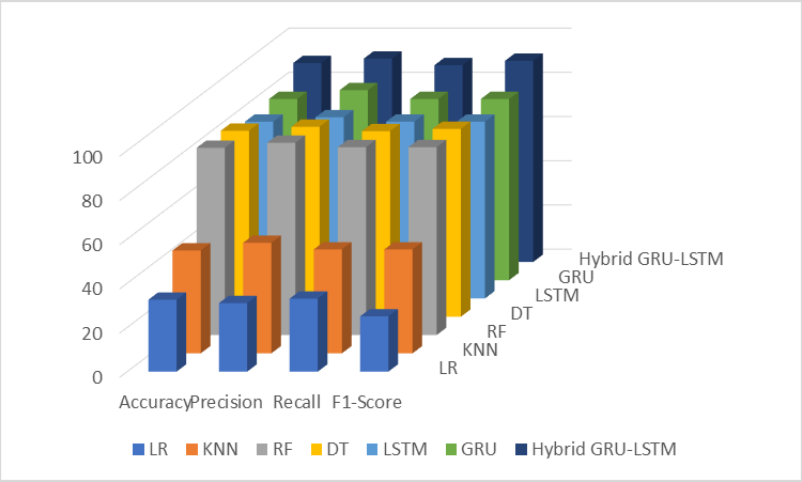

Figure 5 Evaluation comparison graph

6. Conclusion of the proposed work with future prospects

In conclusion, the proposed hybrid GRU-LSTM model demonstrates a significant advancement in real-time threat detection for Industrial Internet of Things (IIoT) environments. By combining the strengths of Gated Recurrent Units (GRUs) and Long Short-Term Memory (LSTM) networks, this model effectively captures both short-term and long-term dependencies in sequential data, resulting in superior performance metrics compared to traditional models. The high accuracy, precision, recall, and F1-score achieved by the hybrid model highlight its robustness and reliability in identifying potential security threats, thereby enhancing the overall security framework of IIoT systems. The promising results of this study pave the way for several future research directions. Firstly, further optimization of the hybrid model can be explored, including fine-tuning hyperparameters and experimenting with different network architectures to enhance performance. Additionally, integrating other advanced techniques such as attention mechanisms could further improve the model's ability to focus on the most critical parts of the input sequence.

Another important future direction is the application of the hybrid model to a broader range of IIoT use cases, including smart grids, industrial automation, and connected healthcare systems. Each of these domains presents unique challenges and requires tailored security solutions. Moreover, the

scalability and efficiency of the model can be evaluated in large-scale deployments, ensuring it can handle the high volume of data generated by extensive IIoT networks.

This research not only contributes a powerful tool for IIoT security but also opens up multiple pathways for future innovation and development in the field of cybersecurity for connected industrial systems.

Reference

[1] M. Aghvamipanah, M. Amini, C. Artho, and M. Balliu, “Activity Recognition Protection for IoT Trigger-Action Platforms.”

[2] A. El Ahmadi, O. Abdoun, and E. K. Haimoudi, “A Comprehensive Study of Integrating AI-Based Security Techniques on the Internet of Things BT - International Conference on Advanced Intelligent Systems for Sustainable Development,” 2023, pp. 348–358.

[3] S. P. V. V. Reddy, S. P. Manonmani, C. Anitha, D. Jaganathan, R. Reena, and M. Suresh, “MLIDS: Revolutionizing of IoT based Digital Security Mechanism with Machine Learning Assisted Intrusion Detection System,” in *2024 International Conference on Automation and Computation (AUTOCOM)*, 2024, pp. 277–282, doi: 10.1109/AUTOCOM60220.2024.10486179.

[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,” *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8852–8859, 2020, doi: 10.1109/JIOT.2020.2996425.

[5] A. Ur-Rehman, I. Gondal, J. Kamruzzaman, and A. Jolfaei, “Sensitivity Analysis for Vulnerability Mitigation in Hybrid Networks,” *Electronics*, vol. 11, no. 2. 2022, doi: 10.3390/electronics11020238.

[6] S. Zaman *et al.*, “Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey,” *IEEE Access*, vol. 9, pp. 94668–94690, 2021, doi: 10.1109/ACCESS.2021.3089681.

[7] E. Staddon, V. Loscri, and N. Mitton, “Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey,” *Applied Sciences*, vol. 11, no. 16. 2021, doi: 10.3390/app11167228.

[8] A. Sundas, S. Badotra, S. Bharany, A. Almogren, E. M. Tag-ElDin, and A. U. Rehman, “HealthGuard: An Intelligent Healthcare System Security Framework Based on Machine Learning,” *Sustainability*, vol. 14, no. 19. 2022, doi: 10.3390/su141911934.

[9] A. S. and S. D., “Understanding insiders in cloud adopted organizations: A survey on taxonomies, incident analysis, defensive solutions, challenges,” *Futur. Gener. Comput. Syst.*, vol. 158, pp. 427–446, 2024, doi: https://doi.org/10.1016/j.future.2024.04.033.

[10] M. Al-Fawa’reh, M. Al-Fayoumi, S. Nashwan, and S. Fraihat, “Cyber threat intelligence using PCA-DNN model to detect abnormal network behavior,” *Egypt. Informatics J.*, vol. 23, no. 2, pp. 173–185, 2022, doi: https://doi.org/10.1016/j.eij.2021.12.001.

[11] S. Algarni *et al.*, “Blockchain-Based Secured Access Control in an IoT System,” *Applied Sciences*, vol. 11, no. 4. 2021, doi: 10.3390/app11041772.

[12] R. Alkanhel *et al.*, “Network Intrusion Detection Based on Feature Selection and Hybrid Metaheuristic Optimization,” *Comput. Mater. Contin.*, vol. 74, no. 2, pp. 2677–2693, 2023, doi: 10.32604/cmc.2023.033273.

[13] P. Dhillon and M. Singh, “Internet of things attacks and countermeasure access control techniques: A review,” *Int. J. Appl. Eng. Res.*, vol. 14, no. 7, pp. 1689–1698, 2019.

[14] N. I. Haque, M. Ngouen, M. A. Rahman, S. Uluagac, and L. Njilla, “SHATTER: Control and Defense-Aware Attack Analytics for Activity-Driven Smart Home Systems,” in *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2023, pp. 1–13, doi: 10.1109/DSN58367.2023.00015.

[15] S. A. Khowaja and P. Khuwaja, “Q-learning and LSTM based deep active learning strategy for malware defense in industrial IoT applications,” *Multimed. Tools Appl.*, vol. 80, no. 10, pp. 14637–14663, 2021, doi: 10.1007/s11042-020-10371-0.

[16] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Networks*, vol. 84, pp. 124–147, 2019, doi: https://doi.org/10.1016/j.adhoc.2018.10.002.

[17] J. Mante (Khurpade), P. Patil, M. Dhotay, and S. Budhavale, "A Hybrid Ensemble Machine Learning Approach (EHML) for DDOS Attack Detection in Smart City Network Traffic BT - Intelligent Systems for Smart Cities," 2024, pp. 53–69.

[18] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, "Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2. 2023, doi: 10.3390/jsan12020029.

[19] M. Panahnejad and M. Mirabi, "APT-Dt-KC: advanced persistent threat detection based on kill-chain model," *J. Supercomput.*, vol. 78, no. 6, pp. 8644–8677, 2022, doi: 10.1007/s11227-021-04201-9.