Fusing Deep Learning Techniques for Intrusion Detection in Smart Grids

Rahul R.[1], Sindhu P.[2], G. Naveen Sundar[3], R. Venkatesan [4 *]

[1,3,4] Department of Computer Science and Engineering ,Karunya Institute of Technology and Sciences

[2] Department of Computer Science and Engineering ,Rajiv Gandhi College of Engineering, Anna University

Emails: rahul22@karunya.edu.in; sindhupandi26@gmail.com; gnaveensundar@gmail.com
rlvenkei2000@gmail.com *

Abstract

Smart grids, pivotal in modern energy distribution, confront a mounting cybersecurity threat landscape due to their increased connectivity. This study introduces a novel hybrid deep learning approach designed for robust intrusion detection, addressing the imperative to fortify the security of these critical infrastructures. Renamed as "Intrusion Detection for Smart Grid Using a Hybrid Deep Learning Approach," the study amalgamates Conv1D for spatial feature extraction, MaxPooling1D for dimensionality reduction, and GRU for modeling temporal dependencies. The research leverages the Edge-IIoTset Cyber Security Dataset, encompassing diverse layers of emerging technologies within smart grids and facilitating a nuanced understanding of intrusion patterns. Over 10 types of IoT devices and 14 attack categories contribute to the dataset's richness, enhancing the model's training and evaluation. The proposed hybrid model's architecture is detailed, emphasizing the synergy of convolutional and recurrent neural networks in addressing complex intrusion scenarios. This research not only contributes to the evolving field of intrusion detection in smart grids but also sets the stage for creating adaptive security systems. The convergence of a hybrid deep learning approach with a comprehensive cyber security dataset marks a significant stride towards fortifying smart grids against evolving cybersecurity threats. The proposed model achieves 98.20 percentage.

Keywords: Smart Grid Security; Intrusion detection; Cyberattacks; Convolutional Neural Networks(CNN); Gated Recurrent Unit GRU; Network Security; Deep Learning.

1. Introduction:

The proliferation of smart grids, an integral facet of contemporary infrastructure, has ushered in unparalleled efficiencies in energy management and distribution. However, this connectivity to the internet exposes smart grids to an escalating array of cybersecurity threats, posing grave risks to the integrity of cyber-physical systems. The potential for attackers to manipulate readings, disrupt operations, and even induce robust security measures to safeguard these critical systems. In response to the imperative for heightened security in smart grids, this research introduces a novel deep learning model, CMGFD-DL, tailored for intrusion detection. The acronym denotes the layers, each designed to fulfill specific functions within the model. The integration of convolutional and recurrent layers aims to enhance the system's ability to detect and cross malicious activities. Central to this study is the utilization of the Edge-IIoT set Cyber Security Dataset, a comprehensive repository structured across seven layers of emerging technologies. This paper uses Virtualization, Blockchain Network, Fog Computing, SDN, Edge Computing, and IoT/IIoT , this dataset provides a rich source for evaluating intrusion detection mechanisms in smart grid environments. In response to the escalating cybersecurity threats faced by smart grids, a significant body of research has explored innovative approaches to enhance intrusion detection systems. Several studies, including those by Cao et al. [12] and Odeh and Taleb [16]. Moreover, the work by Soliman et al. [18]

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

on Industrial Internet of Things (IIoT) networks emphasizes the role of singular value decomposition and synthetic minority oversampling in achieving outstanding accuracy rates. Ben Said et al. [19], focuses on addressing security challenges in Software-Defined Networks (SDNs). The proposed model, combining CNN and bidirectional LSTM networks, showcases heightened efficiency in intrusion detection. The results across various studies consistently underscore the necessity of employing advanced deep learning techniques. Furthermore, the study by Henry et al. [15] specifically targets the challenges posed by IoT devices demonstrating the adaptability of such architectures in addressing the unique characteristics of IoT-related threats. These findings collectively emphasize the critical need for sophisticated intrusion detection models tailored to the intricacies of smart grids. The proposed CMGFD-DL model, incorporating ConvID, MaxPooling, GRU, Flatten, and Dense layers, seeks to contribute to this growing body of research by harnessing the strengths of both convolutional and recurrent layers. By integrating insights from these pioneering studies, our research positions itself at the forefront of the evolving landscape of intrusion detection for smart grids, aiming to fortify these critical systems against emerging cybersecurity challenges.

2. Related works:

In the landscape of smart grid security, existing works have predominantly centered around traditional intrusion detection methods, relying on rule-based systems and signature-based approaches. While efficient to some extent, these approaches often struggle to adapt to the evolving and sophisticated nature of cyber threats. Furthermore, the dynamic and complex nature of smart grids demands a more nuanced and robust solution. Recent studies have acknowledged the limitations of conventional methods and have explored the potential of machine learning techniques. However, a comprehensive hybrid deep learning approach remains underexplored in the topic of smart grid intrusion detection. In addressing the multifaceted challenges within smart grid cybersecurity, recent research has witnessed a proliferation of innovative approaches. Feng Zhai et al. [1] propose CNN–GRU–FL, a decentralized solution tackling the inherent conflict between data privacy and network security in smart grid business units. Ulaa AlHaddad et al. [2] lay the relation for improved the security of Smart Grid communication infrastructure by proposing a pioneering hybrid deep-learning method. This approach specifically targets the detection of DDOS attacks. The researchers leverage the combined power of Convolutional Neural Network (CNN) and Recurrent Gated Unit (GRU) algorithms to fortify the Smart Grid against potential threats. Kilichev et al. [3] contribute to the domain of intrusion detection systems (IDS) by introducing an model tailored for Internet of Things based electric vehicle charging stations. In tandem, Yakubu Imrana et al. [4] contribute to the field by addressing the complex challenge of identifying and preventing malicious network behavior. They introduce a novel technique called CNN-GRU-FF, which involves a double-layer feature extraction and fusion process. Additionally, they propose a modified focal loss function to handle class imbalance in intrusion detection datasets. Through thorough comparative analysis against seven baseline algorithms and existing methods in the field, their research demonstrates the superior performance of the CNN-GRU-FF approach, establishing it as an advanced solution for network intrusion detection.

Shifting focus to a distinct facet of smart grid security, Nasir Ayub et al. [5] delve into the realm of electricity theft, leveraging a dataset sourced from the State Grid Corporation of China (SGCC). The research employs a CNN-GRU-CS model, showcasing its efficacy through simulated results based on real energy consumption data. Remarkably, the CNN-GRU-CS model outperforms alternative approaches by an average of 10%, providing a robust and accurate solution for addressing electricity theft in smart grid environments. DEVINDER KAUR et al. [6] introduce a CNN-Bayesian approach in the context of cyber-physical smart grid (CPSG) systems. Demonstrating superior performance in accuracy, the CNN-Bayesian method stands out as an effective solution for discriminating intrusions in CPSG systems. Muhammed Zekeriya Gunduz et al. [7] propose a hybrid CNN based system for detecting cyber-attacks in Internet of Things-based smart grids. Synthetic datasets, encompassing various attack vectors, are generated, showcasing improved performance in training the hybrid CNN-based detector for accurate classification of honest and malicious consumption patterns. M. Ravinder et al. [8] present an intelligent deep learning approach for detecting anomalies in smart grids, addressing communication challenges within the integrated Information and Communication Technologies (ICT). The anomaly detection model, named "Adaptive Residual RNN with Dilated GRU" demonstrates superior performance in simulations, showcasing a heightened detection rate compared to existing methods and reinforcing the robustness of the smart grid system. J. JITHISH et al. [9] pioneer a Federated Learning (FL)-based anomaly detection scheme in smart grids. The study also highlights the efficiency of FL-based models in terms of resource usage, making them suitable for implementation in resource-constrained environments like

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

smart meters. Jing Gao [10] proposes a network intrusion detection method merging CNN and BiLSTM networks, enhancing the performance of the network intrusion detection system. Ghayth ALMahadin et al. [11] introduce a GRU-based deep learning model for anomaly detection in Vehicular Ad-hoc Networks (VANETs), addressing challenges in intelligent transportation systems. Results show that the GRU-based model outperforms existing methods, achieving superior performance with low false positive rates in network anomaly detection. Collectively, these diverse studies underscore the growing importance of hybrid deep learning, anomaly detection, and federated learning in fortifying smart grids against cybersecurity threats, emphasizing the need for innovative, interdisciplinary solutions to enhance the security posture of smart grid environments. These studies collectively contribute to the evolving landscape of smart grid cybersecurity, demonstrating the versatility and effectiveness of various deep learning architectures and methodologies in addressing complex challenges within this critical domain.

In recent research endeavors, Cao et al. [12] contribute significantly to the domain of intrusion detection with their innovative model that seamlessly integrates CNN and GRU. The proposed model addresses critical challenges related to low accuracy and class imbalance, showcasing its efficacy on diverse datasets such as UNSW_NB15, NSL-KDD, and CIC-IDS2017. Through rigorous evaluation, the study highlights the enhanced performance of their model, providing a valuable contribution to the progress of intrusion detection systems, especially in the context of diverse and complex datasets commonly encountered in cybersecurity research.. Similarly, in their work, Cao et al. [13] propose a network intrusion detection model that combines CNN and bidirectional GRU, strategically targeting issues related to accuracy and false-alarm rates. Through the integration of a hybrid sampling approach and feature selection techniques, the model showcases improved performance in detecting intrusion behaviors across diverse datasets. In a parallel effort, Halbouni et al. [14] focus on the improvement of an efficient intrusion detection system, utilizing CNN for spatial feature extraction and Long Short-Term Memory (LSTM). This hybrid model exhibits high detection rates and accuracy on datasets like CIC-IDS 2017, UNSW-NB15, and WSN-DS. Addressing the critical issue of zero-day attack detection in Intrusion Detection Systems (IDSs), Henry et al. [15] present an approach that combines CNN and GRU. Their proposed methodology signifies a notable improvement in attack detection, as demonstrated on the CICIDS-2017 benchmark dataset. Odeh et al. [16] underscore the crucial role of IoT intrusion detection by presenting an ensemble deep learning framework that integrates CNNs, LSTM, and GRUs. CNN-LSTM and CNN-GRU models prove effective in addressing the evolving cyber threat landscape within IoT environments.

In a distinct domain, Ezhilarasi I and Clement [17] tackle the vulnerability of cognitive radio networks to threats during spectrum sensing. They introduce the use of GRU and Support Vector Machine (SVM) for detection, showcasing the applicability of these methods in enhancing security. Soliman et al. [18] propose an intelligent detection system for cyberattacks in Industrial Internet of Things (IIoT) networks. Their model achieves outstanding accuracy rates for binary and multi-class classification on the ToN_IoT dataset. Ben Said et al. [19] address security challenges in Software-Defined Networks (SDNs) with a hybrid CNN and bidirectional LSTM network for enhanced network intrusion detection. Song et al. [20] introduce an innovative network intrusion detection model, labeled as TGA, which capitalizes on a combination of Temporal Convolutional Network (TCN), Bidirectional GRU (BiGRU), and a self-attention mechanism. This novel approach aims to enhance the system's ability to capture temporal dependencies, bidirectional context, and self-attention patterns, thereby improving its performance in identifying and mitigating network intrusion threats. The study provides a noteworthy contribution to the field, showcasing the efficacy of their proposed model through comprehensive evaluations and comparisons with existing approaches. Their proposed model demonstrates effectiveness in detecting and identifying diverse network attacks. Finally, Ravi et al. [21] highlight the escalating IoT attacks, emphasizing the need for robust security measures in Software-Defined Networking (SDN)-enabled IoT environments. Their proposed feature-fused GRU network outperforms both the GRU model and classical ML based approaches. These collective research endeavors significantly impart to advancing the field of intrusion detection, showcasing the versatility and effectiveness of various deep learning architectures and methodologies in addressing intricate challenges within this critical domain.

Esmaeili et al. explore metainnovations in deep learning-based Intrusion Detection Systems (IDS) for IoT security [22]. They emphasize BiLSTM's effectiveness for binary classification and sequential models for aggressive multiclass attack detection, specifically endorsing BiLSTM for evaluating DDoS attacks in IoT environments due to its reliability and high accuracy. Future research is suggested to investigate the impact of different data processing techniques on IDS, addressing ongoing challenges and enhancing system performance. Chen et al. introduce FCNN-SE, an IDS model addressing feature extraction challenges [23]. FCNN-SE utilizes Fusion CNN (FCNN) for feature extraction and Stacked Ensemble (SE) for classification. Experimental results on the NSL-KDD dataset demonstrate FCNN-SE outperforming other models with the highest overall performance and balanced effectiveness in comparison. Agnew et al. present a co-simulation framework for

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

cybersecurity in power systems [24]. They address threats to communication networks within the smart grid, leveraging machine learning on data from power grids and communication networks. The proposed framework enhances anomaly detection, showcasing superior throughput compared to single-controller frameworks and outperforming existing techniques in attack classification. Mazhar et al. explore the integration of Internet of Things (IoT), Artificial Intelligence (AI), and Smart Grids in the context of smart buildings [25]. The study emphasizes the motivation behind IoT device deployment, focusing on enhancing security and comfort through remote configuration of smart grid monitoring systems. ML methods for building energy demand are discussed.

Stryczek and Natkaniec focus on securing smart grid users with limited resources [26]. They employ ML techniques like LSTM and SVM. Results highlight differences in accuracy, dataset sizes, and suggest the potential for enhanced classification with more analyzed features. Mazhar et al. highlight vulnerabilities in smart grids, focusing on users, communication networks, and administrators [27]. The study discusses risks and flaws affecting the security of these components, proposing security solutions and recommendations to mitigate cyberattack threats in the innovative grid network. Mall et al. present an overview of Authentication and Key Agreement (AKA) protocols [28]. They focus on Physically Unclonable Function (PUF) and its combination with AKA. The article systematically examines and discusses the applications of AKA in IoT, wireless sensor networks, and smart grids, providing a taxonomy and discussing pros and cons. Teng and Ma propose a deep learning layout for intrusion detection in Smart Grid Control Systems (SGCSs) [29]. The model addresses the challenges of asymmetric datasets in SGCS and employs Deep Neural Networks and Decision Tree classifiers. Evaluation using 10-fold cross-validation on real SGCS datasets demonstrates the proposed approach's effectiveness, outperforming traditional schemes like Random Forest and Support Vector Machine in terms of efficiency. Hasan et al. provide a comprehensive review of blockchain implementations in smart grids [30]. They focus on cybersecurity and energy data protection, addressing security issues in smart grid scenarios, and highlighting the potential of big data and blockchain solutions. Starke et al. contribute to Smart Grid security with the introduction of CECD-AS, a cross-layered strategy aimed at fortifying these systems against cyber-threats [31].

By integrating the detection of false Smart Grid (SG) measurement data and inconsistent network inter-arrival times, the proposed approach achieves high accuracy in identifying various types of attacks. Another significant advancement comes from Park et al., who present BPPS, a privacy-preserving authentication scheme tailored for demand response management in Smart Grids [32]. Addressing security concerns associated with smart meters and untrusted wireless communication, BPPS ensures secure mutual authentication through key agreement and maintains the integrity of demand-response data using blockchain technology. The scheme undergoes both informal and formal security analyses, validating its efficacy and robustness within real-world Smart Grid networks.

3. Proposed Method:

The proposed model addresses the critical challenge of intrusion detection within the Smart Grids, emphasizing its application in enhancing cybersecurity for industrial environments. This deep learning-based architecture, tailored for Smart Grid Control Systems (SGCSs), intricately combines CNN and GRU. The objective is to fortify the security of Smart Grids against various cyber threats, including but not limited to affect the integrity and availability. The model's architecture Figure 2 is meticulously designed to accommodate the unique challenges of Smart Grids, with a focus on securing users, communication networks, and administrators. Investing the strengths of CNN for spatial feature extraction and GRU for effective temporal sequence analysis, the model strives to identify and classify potential cyber threats. The utilization of advanced activation functions, such as Leaky Rectified Linear Unit (ReLU), in conjunction with Batch Normalization ensures stability and non-linearity in the feature extraction process. In the experimental phase, the proposed model undergoes rigorous training and testing using a preprocessed dataset specifically tailored for Smart Grid intrusion detection.

The dataset is curated to eliminate redundant features and address class imbalances, reflecting the real-world intricacies of cyber threats in Smart Grids. The training process incorporates essential techniques like early stopping and learning rate reduction, fostering optimal learning while preventing overfitting. The dataset is curated to eliminate redundant features and address class imbalances, reflecting the real-world intricacies of cyber threats in Smart Grids. The training process incorporates essential techniques like early stopping and learning rate reduction, fostering optimal learning while preventing overfitting.The model's evaluation encompasses a suite of performance metrics, including accuracy, F1 score, and false alarm rate, providing a

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

comprehensive understanding of its effectiveness in detecting and classifying cyber threats. The achieved results underscore the model's robustness and reliability, positioning it as a valuable asset in the proactive defense against evolving cybersecurity challenges in Smart Grid environments. This research significantly contributes to the field by presenting a sophisticated intrusion detection system tailored for Smart Grids, acknowledging the distinct characteristics and security requirements of these critical infrastructures. The proposed model stands as a testament to the ongoing efforts to fortify the resilience of industrial systems against cyber threats, raising a secure and reliable Smart Grid ecosystem.

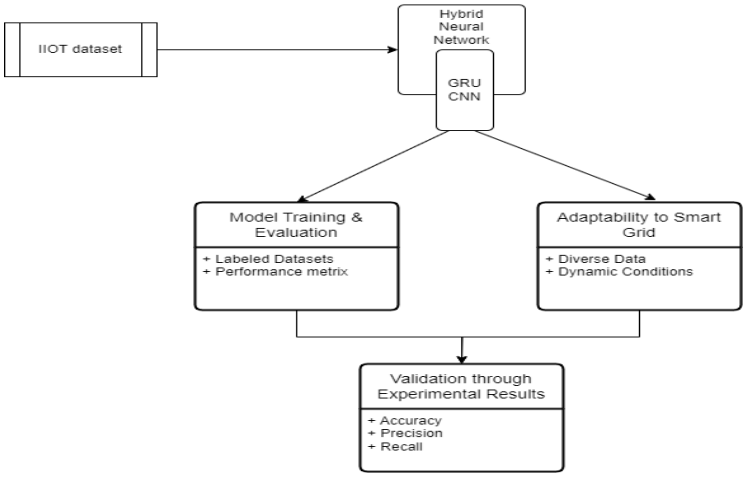

Figure 1: Framework

In the presented intrusion detection model for smart grids, the CNN assumes a crucial role in spatial analysis, extracting valuable features from visual data sources like satellite imagery and surveillance footage. The CNN model is intricately designed to identify anomalies and patterns within the spatial domain, contributing significantly to the hybrid neural network's overall effectiveness. The CNN incorporates multiple convolutional layers for systematic scanning and filtering of input images, each employing convolutional kernels to detect specific features relevant to intrusion detection in agricultural settings. Pooling layers are utilized to downsample spatial dimensions, reducing computational complexity and enhancing the model's ability to generalize patterns across varying spatial contexts. The primary function of the CNN is feature extraction, learning hierarchical representations to recognize spatial patterns associated with normal agricultural activities and identify deviations indicating potential threats. Transfer learning can be employed to fine-tune pre-trained CNN models, leveraging knowledge from large-scale image datasets like ImageNet to improve anomaly detection in smart grid environments. The CNN model is adaptable to diverse visual data sources encountered in smart grids, ensuring robust spatial analysis capabilities across different contexts. Integrated with GRU, the CNN contributes to comprehensive intrusion detection, capturing both spatial and temporal patterns for accurate threat identification. The GRU processes sequences, maintaining internal memory to address the vanishing gradient problem, and features recurrent connections for capturing dependencies over time. In intrusion detection applications, GRUs, including variants like CNN and GRU, are valuable for analyzing sequential data, such as network traffic patterns, to detect anomalies or patterns associated with malicious activities and enhance cybersecurity.

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

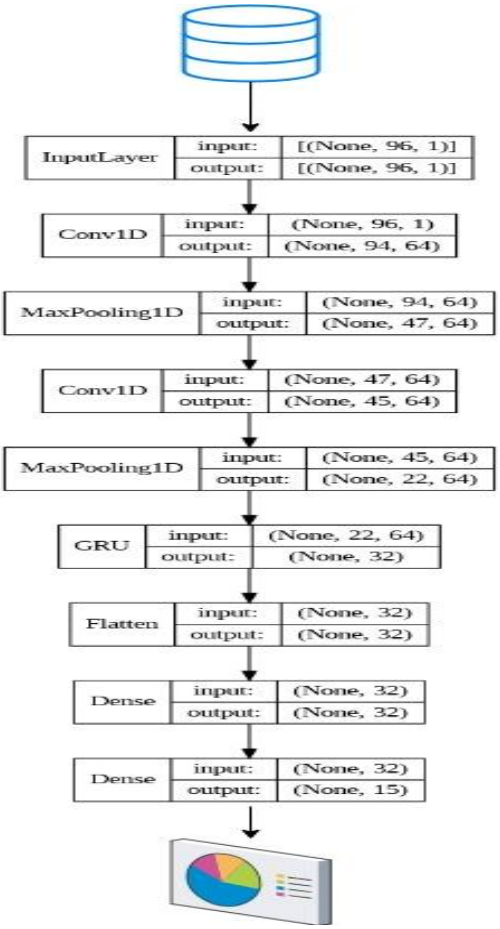

Figure 2: Architecture Diagram

Dataset Used is Edge-IIoTset. It is a novel cyber security dataset for IoT and IIoT applications of smart grid, structured across seven layers featuring emerging technologies to meet key requirements.

4. Results and Discussion

The experimental setup for the proposed IDS model in Smart Grids involves utilizing the Edge-IIoTset Cyber Security Dataset as the foundational dataset. The development and implementation of the deep learning-based model are carried out using the Python programming language within the Google Colab development environment. The choice of Google Colab provides a cloud-based platform, eliminating the need for local computational resources and ensuring scalability. The hardware requirements necessitate a Mac computer with a minimum of 8 GB RAM to facilitate the smooth execution of resource-intensive tasks inherent in training and testing deep learning models. Additionally, GPU accelerators are employed to expedite the computational workload, enhancing the efficiency of the model training process.

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

Table 1: Parameters taken in each layers.

Layer (type)	Output Shape	Param #
conv1d (Conv1D)	(None, 94, 64)	256
max_pooling1d (MaxPooling1D)	(None, 47, 64)	0
conv1d_1 (Conv1D)	(None, 45, 64)	12352
max_pooling1d_1 (MaxPooling1D)	(None, 22, 64)	0
gru (GRU)	(None, 32)	9408
flatten (Flatten)	(None, 32)	0
dense (Dense)	(None, 32)	1056
dense_1 (Dense)	(None, 15)	495

Total params: 23567 (92.06 KB)
Trainable params: 23567 (92.06 KB)
Non-trainable params: 0 (0.00 Byte)

Selecting the optimal dataset for intrusion detection in a smart grid environment depends on several factors. Among the options NSL-KDD, UNSW-NB15, and the Edge IIoT Dataset, each has its merits and drawbacks. The NSL-KDD dataset, stemming from the KDD Cup 99, offers extensive labeled data widely used in the research community, but its limitations in representing real-world scenarios and its aging nature may be considerations. The UNSW-NB15 dataset provides more recent network traffic data with diverse and realistic scenarios, though some labeled attacks may not fully capture the complexity of real-world threats. The Edge IIoT Dataset, designed for Industrial Internet of Things environments, could be particularly relevant to a smart grid setting, but it may lack the scale and variety of more established datasets. Considering the context of smart grid intrusion detection, the Edge IIoT Dataset might be preferable due to its focus on IIoT environments, aligning more closely with the characteristics of a smart grid.

1) ConvID Layer:

$$fConvID(x) = Convolution\ (x, W) + b$$

2) MaxPooling Layer:

$$fMaxPooling(x) = MaxPooling(x)$$

3) GRU Layer:

$$fGRU\ (h_t, x_t) = (1 - Z_t)\ \Theta\ \hat{h}_t + Z_t\ \Theta\ h_{t-1}$$

$$Z_t = \sigma\ (W_z\ .\ [h_{t-1}\ ,\ x_t])$$

$$R_t = \sigma(\ W_r\ .\ [h_{t-1}\ ,\ x_t])$$

$$\hat{H}_t\ = tanh(r_t\ \Theta\ (W_h\ .\ [h_{t-1}, x_t]))$$

4) Flatten Layer:

$$f_{Flatten}\ (x) = Flatten(x)$$

5) Dense Layer:

$$f_{Dence}\ (x) = Activation\ (W\ .\ x + b)$$

These equations collectively define the forward pass of CMGFD-DL. The model's accuracy, as calculated during training and evaluation, is a crucial metric. It's worth noting that the specific formulations of the ConvID, MaxPooling, GRU, Flatten, and Dense layers, as well as the training parameters, would be determined during the model development process. In the context of intrusion detection, the model's performance is rigorously assessed using standard metrics, with accuracy, precision, and recall serving as the primary indicators. The evaluation indicators accuracy (37), Precision (38) and Recall (39) below are the principal indicators to evaluate our model:

[37] Accuracy(A): A = (TP + TN) /(TP + FP + TN + FN)

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

[38] Precision (P): P = TP / (TP + FP)

[39]Recall (R): R = TP / (TP + FN)

In the realm of fifteen-class classification, the ensemble model underwent meticulous evaluation to gauge its proficiency in distinguishing a diverse scope of cybersecurity threats, each characterized by distinct signatures and behavioral patterns. Following an intensive training regimen spanning 10 epochs, the model demonstrated worthy performance, achieving a noteworthy test accuracy of 98.20%, as illustrated in Figure 3. This outcome attests to the model's robustness and capability to effectively categorize a multitude of cybersecurity threats, showcasing its potential utility in complex and varied scenarios.

Comparitive Analysis: Some of the existing models such as CNN, CNN-GRU-CUCKO, RNN, CNN-GRU-FL, Naaive Bayes, GRU-SVM, SEMI-GRU, CNN-LSTM-GRU, Hybrid IDS and Bayesian-CNN gets the following accuracy as shown in the Figue 4 compared with the proposed model. The performance evaluation of the proposed method's GRU layers , EPOCHS and Batch size is 50 and 128.

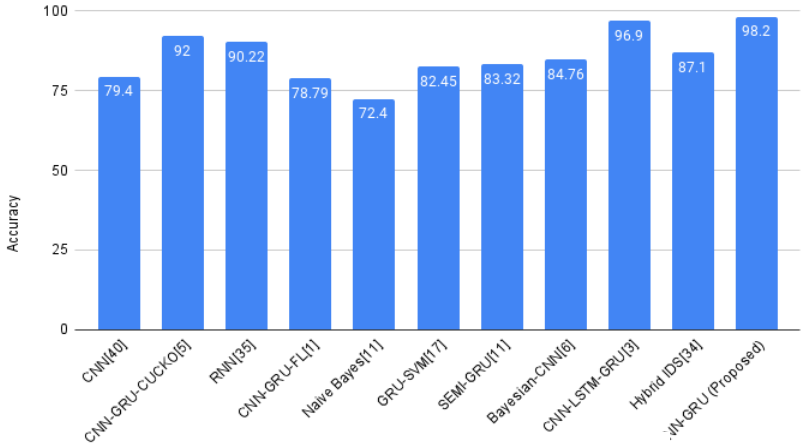

Figure 4: Comparision Graph

5. Conclusion:

This research endeavors to address the escalating cybersecurity threats faced by smart grids through the development of a novel deep learning model for intrusion detection. With an impressive accuracy of 98.20%. This study contributes to the existing body of literature by incorporating insights from seminal works, such as those by Cao et al. [12], Odeh and Taleb [16], Soliman et al. [18], and Ben Said et al. [19], which emphasize the efficacy of hybrid CNN-GRU models, particularly in the context of IIoT networks and SDNs. For future work, there is a promising avenue for the refinement and expansion of the proposed model. Fine-tuning the model architecture based on real-world deployment scenarios, and the exploration of transfer learning techniques could enhance its adaptability to diverse smart grid environments. Additionally, the integration of real-time threat intelligence feeds and continual updates to the model's training data would further fortify its capacity to detect evolving cyber threats. Collaboration with industry stakeholders and cybersecurity experts to validate the model in operational settings is paramount, ensuring its practical applicability and robustness in safeguarding smart grid infrastructures. This research not only contributes a high-accuracy intrusion detection model for smart grids but also sets the stage for future advancements in enhancing the resilience of these critical cyber-physical systems against an ever-evolving threat landscape.

References

[1] Zhai, F., Yang, T., Chen, H., He, B. and Li, S., 2023. Intrusion detection method based on CNN–GRU–FL in a smart grid environment. Electronics, 12(5), p.1164.

[2] AlHaddad, U., Basuhail, A., Khemakhem, M., Eassa, F.E. and Jambi, K., 2023. Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks. Sensors, 23(17), p.7464.

[3] Kilichev, D., Turimov, D. and Kim, W., 2024. Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models. Mathematics, 12(4), p.571.

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

[4] Imrana, Y., Xiang, Y., Ali, L., Noor, A., Sarpong, K. and Abdullah, M.A., 2024. CNN-GRU-FF: a double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. Complex & Intelligent Systems, pp.1-18.
[5] Ayub, N., Ali, U., Mustafa, K., Mohsin, S.M. and Aslam, S., 2022. Predictive data analytics for electricity fraud detection using tuned cnn ensembler in smart grid. Forecasting, 4(4), pp.936-948.
[6] Kaur, D., Anwar, A., Kamwa, I., Islam, S., Muyeen, S.M. and Hosseinzadeh, N., 2023. A Bayesian deep learning approach with convolutional feature engineering to discriminate cyber-physical intrusions in smart grid systems. IEEE Access, 11, pp.18910-18920.
[7] Gunduz, M.Z. and Das, R., 2024. Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns. Sensors, 24(4), p.1148.
[8] Scholar, R., 2024. Optimizing Anomaly Detection in Smart Grids with Modified FDA and Dilated GRU-based Adaptive Residual RNN.
[9] Jithish, J., Alangot, B., Mahalingam, N. and Yeo, K.S., 2023. Distributed anomaly detection in smart grids: a federated learning-based approach. IEEE Access, 11, pp.7157-7179.
[10] Gao, J., 2022. Network intrusion detection method combining CNN and BiLSTM in cloud computing environment. Computational intelligence and neuroscience, 2022.
[11] ALMahadin, G., Aoudni, Y., Shabaz, M., Agrawal, A.V., Yasmin, G., Alomari, E.S., Al-Khafaji, H.M.R., Dansana, D. and Maaliw, R.R.,2023. VANET Network Traffic Anomaly Detection Using GRU-Based Deep Learning Model. IEEE Transactions on Consumer Electronics.
[12] Cao, B., Li, C., Song, Y., Qin, Y. and Chen, C., 2022. Network intrusion detection model based on CNN and GRU. Applied Sciences, 12(9), p.4184.
[13] Cao, B., Li, C., Song, Y. and Fan, X., 2022. Network intrusion detection technology based on convolutional neural network and BiGRU. Computational Intelligence and Neuroscience, 2022.
[14] Halbouni, A., Gunawan, T.S., Habaebi, M.H., Halbouni, M., Kartiwi, M. and Ahmad, R., 2022. CNN-LSTM: hybrid deep neural network for network intrusion detection system. IEEE Access, 10, pp.99837-99849.
[15] Henry, A., Gautam, S., Khanna, S., Rabie, K., Shongwe, T., Bhattacharya, P., Sharma, B. and Chowdhury, S., 2023. Composition of hybrid deep learning model and feature optimization for intrusion detection system. Sensors, 23(2), p.890.
[16] Odeh, A. and Abu Taleb, A., 2023. Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection. Applied Sciences, 13(21), p.11985.
[17] Clement, J.C., 2023. GRU-SVM Based Threat Detection in Cognitive Radio Network. Sensors, 23(3), p.1326.
[18] Soliman, S., Oudah, W. and Aljuhani, A., 2023. Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alexandria Engineering Journal, 81, pp.371-383.
[19] Said, R.B., Sabir, Z. and Askerzade, I., 2023. CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software Defined Networking with Hybrid Feature election. IEEE Access.
[20] Song, Y., Luktarhan, N., Shi, Z. and Wu, H., 2023. TGA: a novel network intrusion detection method based on TCN, BiGRU and attention mechanism. Electronics, 12(13), p.2849.
[21] Ravi, V., Chaganti, R. and Alazab, M., 2022. Deep learning feature fusion approach for an intrusion detection system in SDN-based IoT networks. IEEE Internet of Things Magazine, 5(2), pp.24-29.
[22] Esmaeili, M., Goki, S.H., Masjidi, B.H.K., Sameh, M., Gharagozlou, H. and Mohammed, A.S., 2022. Ml-ddosnet: Iot intrusion detection based on denial-of-service attacks using machine learning methods and nsl-kdd. Wireless Communications and Mobile Computing, 2022.
[23] Chen, C., Song, Y., Yue, S., Xu, X., Zhou, L., Lv, Q. and Yang, L., 2022. Fcnn-se: An intrusion detection model based on a fusion CNN and stacked ensemble. Applied Sciences, 12(17), p.8601.
[24] Agnew, D., Aljohani, N., Mathieu, R., Boamah, S., Nagaraj, K., McNair, J. and Bretas, A., 2022. Implementation aspects of smart grids cyber-security cross-layered framework for critical infrastructure operation. Applied Sciences, 12(14), p.6868.
[25] Mazhar, T., Irfan, H.M., Haq, I., Ullah, I., Ashraf, M., Shloul, T.A., Ghadi, Y.Y., Imran and Elkamchouchi, D.H., 2023. Analysis of challenges and solutions of IoT in smart grids using AI and machine learning techniques: A review. Electronics, 12(1), p.242.
[26] Stryczek, S. and Natkaniec, M., 2022. Internet Threat Detection in Smart Grids Based on Network Traffic Analysis Using LSTM, IF, and SVM. Energies, 16(1), p.329.
[27] Mazhar, T., Irfan, H.M., Khan, S., Haq, I., Ullah, I., Iqbal, M. and Hamam, H., 2023. Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. Future Internet, 15(2), p.83.

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024

[28] Mall, P., Amin, R., Das, A.K., Leung, M.T. and Choo, K.K.R., 2022. PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey. IEEE Internet of Things Journal, 9(11), pp.8205-8228.
[29] Teng, T. and Ma, L., 2022. Deep learning-based risk management of financial market in smart grid. Computers and Electrical Engineering, 99, p.107844.
[30] Hasan, M.K., Alkhalifah, A., Islam, S., Babiker, N.B., Habib, A.A., Aman, A.H.M. and Hossain, M.A., 2022. Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations. Wireless Communications and Mobile Computing, 2022, pp.1-26.
[31] Starke, A., Nagaraj, K., Ruben, C., Aljohani, N., Zou, S., Bretas, A., McNair, J. and Zare, A., 2022. Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security. IET Smart Grid, 5(6), pp.398-416.
[32] Park, K., Lee, J., Das, A.K. and Park, Y., 2022. BPPS: Blockchain-enabled privacy-preserving scheme for demand-response management in smart grid environments. IEEE Transactions on Dependable and Secure Computing, 20(2), pp.1719-1729.
[33] Ferrag, M.A., Friha, O., Hamouda, D., Maglaras, L. and Janicke, H., 2022. Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access, 10, pp.40281-40306.
[34] Patel, H.D., 2023. A Hybrid IDS using Machine Learning and Semantic Rules for Modern Power Systems to Detect Cyber-Attacks (Doctoral dissertation, Dublin, National College of Ireland).
[35] Salih, K.M.M.; Ibrahim, N.B. Enhancing IoT Forensics through Deep Learning: Investigating Cyber-Attacks and Analyzing Big Data for Improved Security Measures. In Proceedings of the 2023 4th International Conference on Big Data Analytics and Practices (IBDAP), Bangkok, Thailand, 25–27 August 2023; pp. 1–8.
[36] Soliman, S., Oudah, W. and Aljuhani, A., 2023. Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alexandria Engineering Journal, 81, pp.371-383.
[37] M. Latah and L. Toker, ‘‘An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks,’’ CCF Trans. Netw., vol. 3, nos. 3–4, pp. 261–271, Dec. 2020, doi: 10.1007/s42045-020-00040-z.
[38] M. S. ElSayed, N.-A. Le-Khac, M. A. Albahar, and A. Jurcut, ‘‘A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique,’’ J. Netw. Comput. Appl., vol. 191, Oct. 2021, Art. no. 103160.
[39] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, ‘‘Survey on SDN based network intrusion detection system using machine learning approaches,’’ Peer-Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, Mar. 2019, doi: 10.1007/s12083-017-0630-0.
[40] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," in IEEE Access, vol. 6, pp. 3491-3508, 2018, doi:10.1109/ACCESS.2017.2782159
[41] Sathya Preiya V, Kumar VDA. Deep Learning-Based Classification and Feature Extraction for Predicting Pathogenesis of Foot Ulcers in Patients with Diabetes. *Diagnostics*. 2023; 13(12):1983. https://doi.org/10.3390/diagnostics13121983.
[42] Balakrishnan C, Ambeth Kumar VD. IoT-Enabled Classification of Echocardiogram Images for Cardiovascular Disease Risk Prediction with Pre-Trained Recurrent Convolutional Neural Networks. Diagnostics (Basel). 2023 Feb 18;13(4):775. doi: 10.3390/diagnostics13040775. PMID: 36832263; PMCID: PMC9955174.
[43] Hemamalini, Selvamani, and Visvam Devadoss Ambeth Kumar. 2022. "Outlier Based Skimpy Regularization Fuzzy Clustering Algorithm for Diabetic Retinopathy Image Segmentation" *Symmetry* 14, no. 12: 2512. https://doi.org/10.3390/sym14122512.
[44] Kumar, V.D.A., Sharmila, S., Kumar, A. *et al.* A novel solution for finding postpartum haemorrhage using fuzzy neural techniques. *Neural Comput & Applic* **35**, 23683–23696 (2023). https://doi.org/10.1007/s00521-020-05683-z
[45] V. D. A. Kumar, M. Raghuraman, A. Kumar, M. Rashid, S. Hakak and M. P. K. Reddy, "Green-Tech CAV: Next Generation Computing for Traffic Sign and Obstacle Detection in Connected and Autonomous Vehicles," in *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1307-1315, Sept. 2022, doi: 10.1109/TGCN.2022.3162698.
[46] Abhishek Kumar, Kamred Udham Singh, Visvam Devadoss Ambeth Kumar, Tapan Kant, Abdul Khader Jilani Saudagar, Abdullah Al Tameem, Mohammed Al Khathami, Muhammad Badruddin Khan, Mozaherul Hoque Abul Hasanat, Khalid Mahmood Malik, " Robust Watermarking Scheme for NIfTI Medical Images", Vol.71, No.2, 2022, pp.3107-3125, doi:10.32604/cmc.2022.022817
[47] V.D.Ambeth Kumar and M.Ramakrishan (2013), “Temple and Maternity Ward Security using FPRS” in the month of May for the Journal of Electrical Engineering & Technology (JEET) ,Vol. 8, No. 3, PP: 633-637.

Doi: https://doi.org/10.54216/FPA.160105
Received: July 18, 2023 Revised: November 24, 2023 Accepted: April 21, 2024