ISSN: 2093-5374 / E-ISSN: 2093-5382

An Integrated Approach for Intrusion Detection in Intelligent Grid Computing Networks Using Machine Learning

K. Meenakshi[1*], Dr.M. Naga Raju[2], Dr. Channabasamma Arandi[3], Dr.D.V. Lalitha Parameswari[4], Dr.R.N. Ashlin Deepa[5], and Veena Potdar[6]

[1*]Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chengalpet District, Tamil Nadu, India. meenaksk@srmist.edu.in, https://orcid.org/0000-0002-5428-6353

[2]Associate Professor, Department of CSE, GITAM School of Technology, GITAM (Deemed to be University), Nagadenahalli, Doddabalapur, Bengaluru, India. nmysore2@gitam.edu, https://orcid.org/0000-0003-0970-0911

[3]Computer Science Department, Koneru Lakshmaiah Education Foundation, Bowrampet, Hyderabad, Telangana, India. channabasamma.ar@gmail.com, https://orcid.org/0000-0003-4689-0638

[4]Computer Science Department, G. Narayanamma Institute of Technology and Science, Hyderabad, India. dvlalitha@gnits.ac.in, https://orcid.org/0000-0002-4283-2193

[5]Computer Science Department, Goksraju Rangaraju Institute of Engineering and Technology, Hyderabad, India. rndeepa.pradeep@gmail.com, https://orcid.org/0000-0002-1742-7516

[6]Assistant Professor, Department of CSE, Dr. Ambedkar Institute of Technology, Outer Ring Road, Mallathahalli, Bangalore, India. veenapotdar@gmail.com, https://orcid.org/0000-0003-3006-688X

Received: July 31, 2024; Revised: September 11, 2024; Accepted: October 09, 2024; Published: December 30, 2024

Abstract

Intelligent Grid (IG) systems improve the usability of old energy networks, but they can still be hacked in many ways. Intruders can get into the system through these holes, risking IG networks' safety and privacy. An Intrusion Detection System (IDS) keeps services safe and secure in an IG setting. With the help of Machine Learning (ML) techniques and characteristics, this work shows an IDS for IG platforms. The categorization algorithm comprises a Convolutional Neural Network (CNN) and a Gated Recurrent Unit (GRU). The research uses Precision, Intrusion Detecting Rate (IDR), and False Alarming Ratio (FAR) to rate how well the suggested approach works. It turns out that the Random Forest (RF) and Neural Network (NN) algorithms did outperform the others. The study found that the KDD-99 records had a False Alarm Rate (FAR) of 7.29%, and the NSL-KDD records had a FAR of 7.31%. 88.68% of the time, both methods find things, and 90.87% of the time, they confirm that they are correct.

Keywords: Intrusion Detection System, Machine Learning, Grid Computing, Smart Grid.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 15, number: 4 (December), pp. 313-324. DOI: *10.58346/JOWUA.2024.I4.020*

*Corresponding author: Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chengalpet District, Tamil Nadu, India.

1 Introduction

Electrical system engineering and information and communication technology (ICT) are combined in the Intelligent Grid (IG) (Moreno Escobar et al., 2021). Its goal is to fix many significant issues with the power grid, including wasting energy, lowering demand, and ensuring the best use of facilities. The typical electrical grid converts just one-third of fuel energy into electricity, with 7% of generation lost during transportation and 25% of producing capacity utilized to satisfy peak needs. The principal function of IG is to furnish utility firms with comprehensive visibility and extensive control offerings, together with enhanced communication skills, to facilitate interaction and execute electrical transactions throughout the grid. This fresh reality will allow power companies to implement an intelligent layer atop their present facilities and systems, yet it presents significant cybersecurity concerns and obstacles that might lead to cascading impacts and catastrophic outcomes for the whole electrical grid.

Cyber assaults on IG systems encompass control signal incidents, measurement assaults, and control-signal-measurement assaults. Common risks hindering data availability include floods, route damage, selective transmission, wormhole assaults, Byzantine assaults, and Denial-of-Service (DoS) assaults (Chaganti et al., 2022). Security measures can often be categorized into two primary strategies: preventative techniques and detection methods. Prevention approaches seek to safeguard network data against interception, with encryption commonly employed. Identification approaches are designed to identify intruders, encompassing signature- and anomaly-based identification. The previous contrasts the observed assault patterns with established ones. The latter contrasts network traffic characteristics with standard ones, where any deviation from regular traffic indicates the existence of an attacker (Anny Leema et al., 2024).

Machine Learning (ML) methods are often employed to recognize and determine diverse attack variants (Aljuhani, 2021). This study implements several ML techniques to categorize network packets as harmful or regular. This research presents an original contribution: Alteration of loads in Particle Swarm Optimization (PSO) techniques enables the suggested balanced PSO to identify optimum features from databases, resulting in Intrusion Detection Rates (IDR), enhanced accuracy, and reduced False Alarm Rates (FAR) (Basnet et al., 2019). This study utilizes two databases: NSL-KDD and KDD-99. After choosing data sets, several preprocessing procedures are implemented on both databases (Fung, 2011). Data sets are standardized by the min-max standardization approach to scale the data. Following normalizing the data, data encoding is executed to transform nominal values into numeric values, as ML operates on numeric information. The efficacy of the suggested system is assessed based on accuracy, IDR, and FAR. The findings indicate that the Random Forest (RF) and Neural Network (NN) classifications have outperformed others (Banumathy et al., 2023). The research attained a 7.29% false alert rate on the KDD-99 dataset and a 7.31% false alarm rate on the NSL-KDD database. Both databases' mean recognition rate and validation accuracy are 88.68% and 90.87%.

2 Background

Numerous studies investigate the security concerns associated with IG. The research offers an extensive survey of IG's Intrusion Detection System (IDS) technologies. This research provides essential background on IG design aspects and their interactions (Liu et al., 2021). A comprehensive examination of IDS systems ensues, evaluating the design and the possible detection groups: (a) signature-based identification, (b) anomaly-based identification, and (c) specification-based identification. The needs of IDS for IG are immediately outlined, followed by a complete examination of 37 pertinent IDS. The analyzed IDS targets explicitly the protection of (a) the whole IG ecosystem, (b) Automated Metering

Instrumentation (AMI), (c) substations, (d) synchrophasors, and (e) SCADA networks. This review outlines the deficiencies and constraints of the existing IDS and suggests potential research avenues in this domain.

The authors say these problems can be fixed by adding a vital checking service part to protect against Distributed Denial of Service (DDoS) threats (Hasan et al., 2023). A test scenario in a network for managing energy shows that the suggested security protection works well. Testing revealed that the design may render things better and more valuable in the real world.

An approach was shown for selection that employed both flow and variable polling. The Snort IDS was paired with a Deep Learning (DL) system built up of Stacked Automatic Encoders (SAE) (D'Angelo & Palmieri, 2021). Using the adaptability of software-defined networks (SDN) makes network design easier. It doesn't need any apps or tools from outside sources. It has been measured and found that the recommended approach is better at discovering things than flexible tracking. About 71% of the time, it finds the right thing, and less than 15% of the time, it finds the wrong thing. This is called its True Positive Rate (TPR). This study makes it more straightforward to spot DDoS threats in Internet of Things (IoT) devices by mixing the good things about SDN and DL.

A study looked at the extent to which two open-source IDS might frequently spot machines on a network doing bad things (Ayodeji et al., 2020). The research examined a hybrid model that used both SVM and fuzzy logic to get better at recognizing things. With an FPR of 16.2% and a False-Negative Ratio (FNR) of 21.4%, the best outcomes were seen when an improved Support Vector Machine (SVM) was used with the firefly technique. If this is true, then speed has sped up a lot. This study utilized a 10 Gbps network connection and new and enhanced machine learning techniques to look at two IDS side by side and find ways to improve Snort.

It was easier for the model to sort and identify items when a backpropagation NN (BPNN) was employed (Li et al., 2023). The proposed BPNN method was primarily made to find attacks on resources, but it might have been more effective in finding strikes. The main point of the study was to look at the causes of danger. Train Gigabit Consist Systems' data security was put at risk by security risks that were looked into in this research. The training job is to receive essential instructions for leadership from this network. The experts developed a new intrusion detection system (IDS) to defend against many network threats, including IP Scanner, Port Scanner, DoS, and Men in the Median (MITM). The approach worked sufficiently well to identify things 79.54% of the time.

The study wanted to improve the K-Nearest Neighbor (KNN) approach to finding botnet threats in the Internet of Things (Khan et al., 2021). The recommended approach was the most accurate and took the least time to run out of all the tried ones. The main point of this study was that DL and ML can find and sort dangerous network threats. The method uses the best elements of Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) to see patterns in space and time. This renders the approach better at making guesses because it works faster and more accurately. This approach correctly finds up to 82.34% of network dangers, making it fun to identify and combat them in everyday life.

They demonstrated how to employ Spectral Clustering (SC) and Deep Neural Networks (DNN) jointly to do IDS in highly complex network datasets (Balla et al., 2024). The recommended formula works better and lasts longer than other ones. It works better than other ways to find and stop network threats.

The main topic of this study was the significance of IDSs in using Artificial Intelligence (AI) and deep learning (DL) tools like CNNs to keep networks and machines safe. The outcomes of this work are

significant for understanding how CNNs can be used in IDSs. It examines the present state of research and places that will require additional study and work in the future.

3 ML-based IDS System in Intelligent Grid

The research shows an AI-based way to keep the IG system safe using the most effective set of characteristics and AI algorithms. The study aims to create a machine learning system that can rapidly and accurately spot network traffic signals while lowering the False Alarm Rate (FAR) and Detection Rate (DR). Effective feature selection is essential for achieving this aim. This study will use the PSO search method to identify the best characteristics from a specified subset.

This study utilizes the NSL-KDD and KDD-99 databases. The research conducts binary categorization, distinguishing between abnormal and regular, and multiclass categorization to forecast attack types, including DoS, Root to Local attacks (R2L), User to Root attacks (U2R), Probing, and Normal groups, for the KDD-99 and NSL-KDD databases. Following the successful categorization of the assaults, the research does categorization to get the precise designation of the anomaly. The suggested paradigm has six stages. The initial step is information reading, during which the research reads the KDD-99 and NSL-KDD databases sequentially. The second phase is data preparation, during which the research substitutes missing values with the mean, eliminates any anomalies, and normalizes the data to scale the dataset. After normalizing the data, the researcher executed the data encoder to transform non-numeric numbers into numbers. The following data preparation phase is optimum feature selection, executed by PSO. The third involves transmitting ideal attributes to determined ML methods. During the fourth step, the researcher learned several systems using 75% of the information and corresponding labels. Testing is conducted on 25% of the dataset. The fifth stage is the experimental phase, while the sixth is the assessment phase. Figure 1 illustrates the suggested approach.

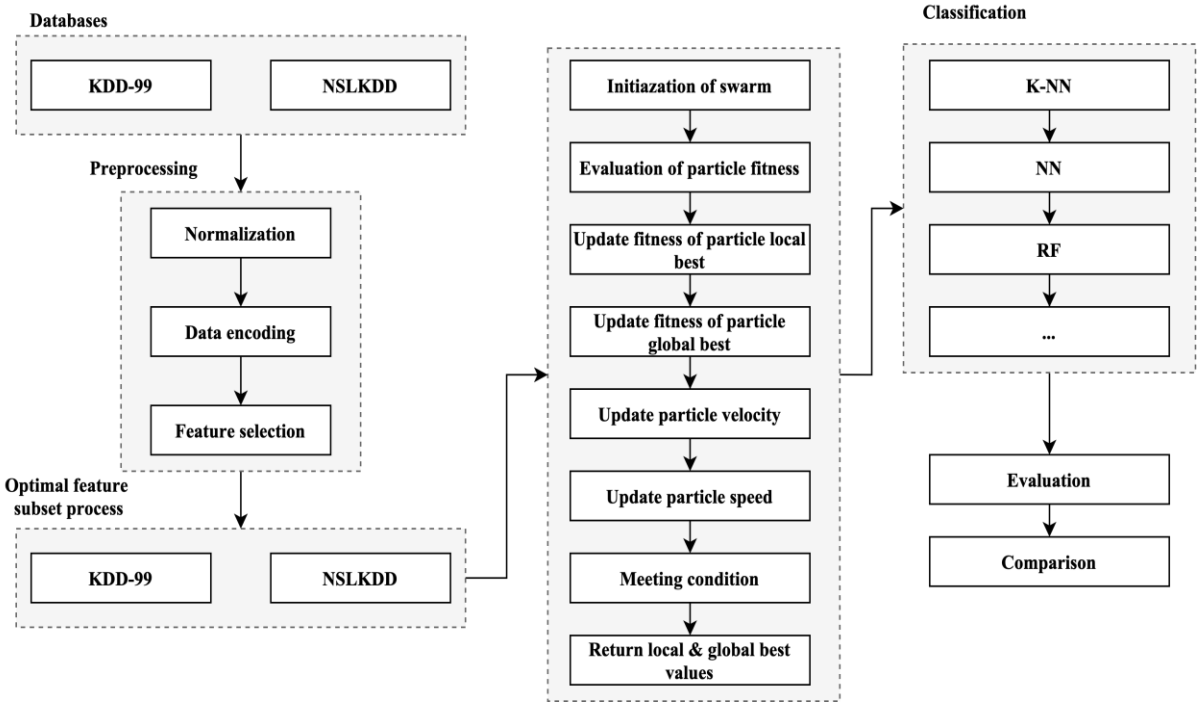

Figure 1: Workflow of the Proposed Method

3.1. Datasets

- **KDD-99 Dataset**

KDD-99 is a prominent dataset utilized in IDS network safety. KDD-99 is a derivative of the DARPA dataset. Created at the MIT research laboratory, it serves as a baseline for IDS architects to assess diverse approaches. The KDD-99 database has 4.9 million records and 40 characteristics, with binary labels and 21 distinct network assaults. Category labels comprise four primary assault types: DoS, Probe, U2R, R2L, and a Normal category. Packets 98k and 398k are utilized for the weird and regular classes to construct ensemble ML classifications for training and testing purposes. Seventy percent of the KDD-99 database is allocated for learning and verification, while the remaining thirty percent is designated for training and verification.

- **NSL-KDD Database**

NSL-KDD is a revised version of the KDD-99 database. NSL-KDD has no redundant values, as seen in the KDD-99 database. NSL-KDD also lacks any conflicting values. NSL-KDD comprises 150k examples and 40 characteristics for comprehensive testing and instruction. The overall count of abnormal and normal messages utilized for training and testing ML algorithms is 72k and 78k, respectively. Seventy percent of the KDD-99 database is allocated for learning, while the remaining thirty percent is designated for evaluation and verification.

3.2. Pre-processing

- **Normalization**

Upon selecting the database, cleansing procedures are executed to eliminate noise and standardize the characteristics. The findings from this study use the min-max standardization strategy, which is superior for scalability and addressing outlier difficulties compared to z-score standardization. Min-max scalability standardizes data within the interval [0, 1]. The formula for min-max standardization is shown below.

$$Z_x = \frac{Y_x - \min(Y)}{\max(Y) - \min(Y)} \quad (1)$$

Equation (1) $Y = \{y_1, y_2, \ldots, y_n\}$ represents the number of characteristics, whereas Y; denotes the characteristic to be standardized, and Z_x signifies the standardized characteristics. All characteristics possess identical quantities and are included under a singular scope.

- **Data Encoding**

Before data encoding, the research removed duplicated and overlapped information from the datasets. Nominal attributes are converted into numerical values since ML algorithms do backend calculations with numeric data instead of nominal data. This step is finalized before relaying data to the suggested approach.

- **Feature Selection**

Following feature standardization, the critical step is feature minimization. Optimal characteristics enhance accuracy and IDR and reduce FAR. The primary objective of optimizing features is to identify subgroups of features that can effectively collaborate with various classifications to yield improved outcomes. This study will use the PSO search strategy to select features. Studies inspired by the flocking

actions of fish and birds led to the development of PSO, primarily an optimization technique. PSO is a potent approach for addressing non-smooth global challenges. The converging rate of PSO is notably high, yielding optimal solutions in a reduced timeframe. Genetic Algorithms (GAs) are employed for optimal selecting features, yielding a favorable detection rate; moreover, their convergence rate could be much higher and deteriorate more if the population topics are utilized. The swarm elements are arbitrarily initiated and introduced to the searching field; by altering the values of velocity and location of the fragments, a suitable subset of characteristics is obtained. Equations (2) and (3) articulate its current location and speed.

$$P_x = \{p_{x1}, p_{x2}, \dots, p_{xN}\} \quad (2)$$

$$D_y = \{d_{y1}, d_{y2}, \dots, d_{yN}\} \quad (3)$$

The dimension of the primary searching area is denoted by N. Continue updating the values for speed and location until the research has the ideal values method. Upon acquiring the ideal characteristics, the system ceases operation.

3.3. Proposed System

The suggested hybrid ML approach for the IDS illustrated in Figure 2 incorporates both CNN and Gated Recurrent Unit (GRU) models. This option was selected due to the prevailing belief that CNNs excel above alternative approaches in properly collecting position-invariant characteristics. The GRU component monitors long-term relationships and utilizes memory cells to extract relevant details from the gathered data. The reset gate is employed to eliminate redundant data. Multiple variables influenced the selection of the GRU algorithm. The computational design had three GRU units and four CNN elements to enhance the system's depth. The primary objective of the convolution tier is to execute its eponymous function, hence generating a feature mapping from the input data through feature extraction. The convolutional core in a NN performs multiplication on the input information. A nonlinear process activates the system. This operation occurs within the convolutional system to get feature translation. The convolution core arbitrarily assigns the weights and biases. Following the conclusion of each CNN tier, a standardization layer and a maximum pooling layer are incorporated. A pooling function identifies the most prominent or representative value for all qualities within a particular area's proximity.

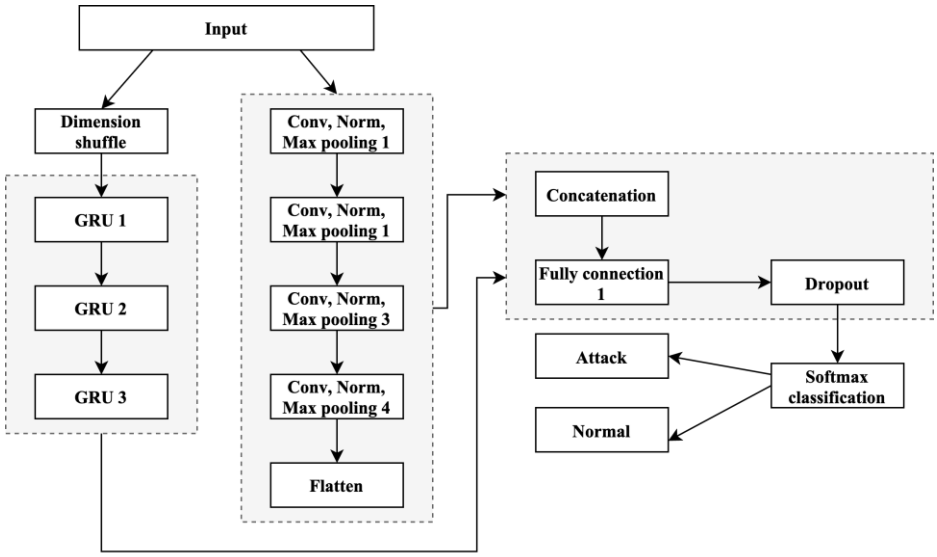

Figure 2: Combined ML Model for IDS in IG

The outputs of the GRUs and CNNs are integrated into the concatenation tier, which also accepts the flattened result from the CNN tiers. After the concatenation tier, two pre-existing interconnected tiers are amalgamated. A dropout tier is incorporated following the last connected tier to prevent overfitting. The SoftMax tier, linked to the categorization layer, transforms the result into a distribution of probabilities. This allows the categorization layer to generate accurate estimates regarding the types of identifiers. The research assessed this approach by implementing it on the NSL-KDD-99 and locally produced datasets, then compared the outcomes using a combined framework of CNN with the GRU models.

3.4. Evaluation Metrics

The suggested approach is evaluated using several performance measures, such as precision, recall, F1-Measure, FAR, DR, and Accuracy. The performance above indicators are based on TPR, FPR, FNR, and True Negative Rate (TNR).

The FAR is the ratio of the ordinary occurrences that are misclassified as belonging to the attack group relative to the occurrences that belong to the attack category in equation (4).

$$FAR = \frac{FPR}{FPR+TNR} \tag{4}$$

Accuracy measures the number of events accurately categorized as belonging to the standard and attack categories. Accuracy is determined by the ratio of correctly classified cases to the overall occurrences, as expressed in Equation (5).

$$A = \frac{TPR+TNR}{TPR+TNR+FPR+FNR} \tag{5}$$

The DR indicates the proportion of accurately identified assaults relative to the overall amount of threats in the database in equation (6).

$$DR = \frac{TP}{TP+FN} \tag{6}$$

Precision aims to assess TPR instances compared to FPR instances in equation (7).

$$P = \frac{TPR}{TPR+FPR} \tag{7}$$

Recall aims to assess TPR items compared to FNR things that remain uncategorized. The mathematical representation of recollection is delineated in Equation (8).

$$R = \frac{TPR}{TPR+FNR} \tag{8}$$

Performance evaluation needs more accuracy and recall; for example, an alternative method is required if one mining method has lower recall but higher precision. The inquiry arises regarding whether the process is superior. This issue is addressed by utilizing the F1-score, which provides a mean of recall and accuracy. The F1-score can be computed as seen in Equation (9).

$$F = \frac{2*P*R}{P+R} \tag{9}$$

4 Simulation Analysis and Outcomes

This section presents the experimental findings of KDD-99 and NSL-KDD. All these tests are conducted on Google Colab. A Core i5 machine with 8 GB of Random Access Memory (RAM) and a 2.4 GHz Central Processing Unit (CPU) is utilized.

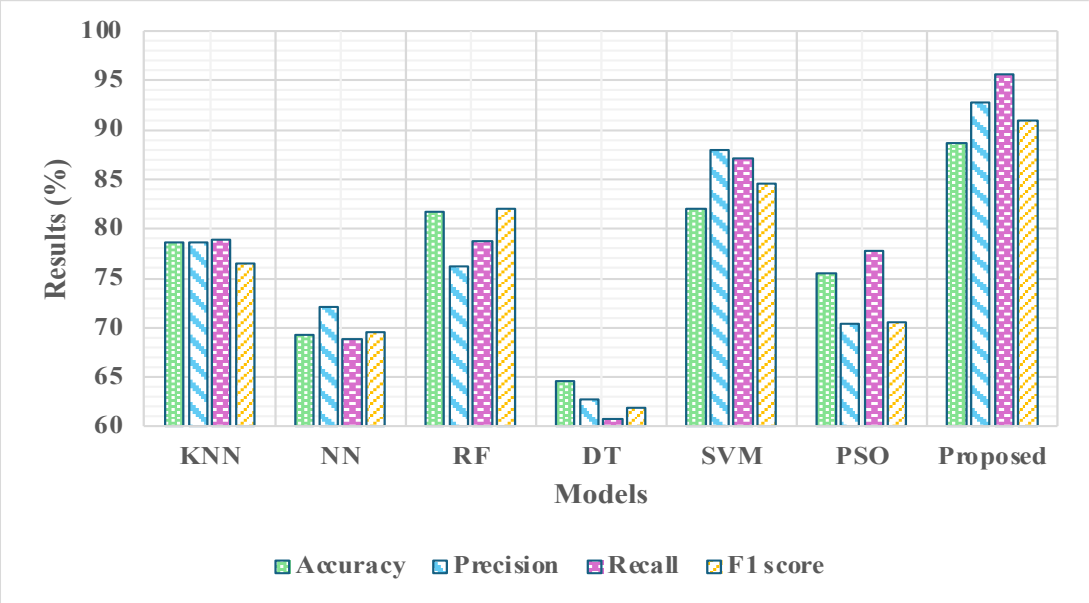

Figure 3: Performance Analysis

The experimental findings are illustrated in Figure 3. The findings indicate that all packages were classified into two main groups: aberrant data and standard information. The anomalous data remained unclassified, and the sampling imbalance posed a lesser issue. In actual applications, the groups of abnormal details must be delineated, necessitating consideration of the impact of sample imbalances on training outcomes in following multi-classification scenarios.

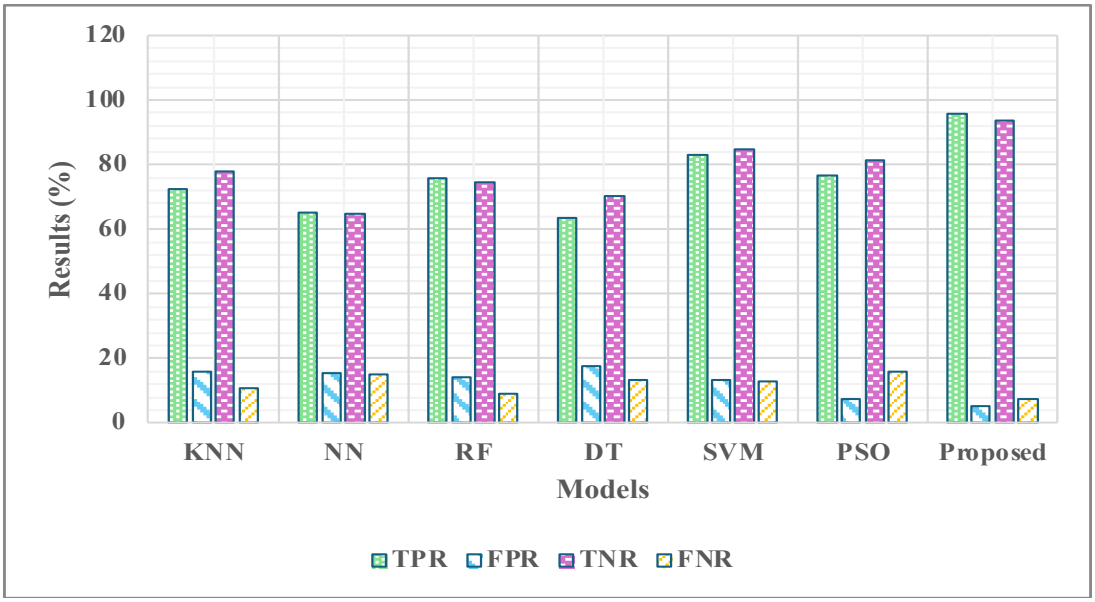

Figure 4: Confusion Matrix for KDD-99 Database

Figure 4 shows the confusion matrix results for the KDD-99 database, showing how different models compare. The suggested method works better than the others because it has the lowest FPR (5.39%) and the highest TPR (95.62%). It also has the lowest FNR (7.29%). SVM also shows competitive metrics but could be better than the proposed method. Different from the suggested method, models like Decision Tree (DT) and NN are less accurate and show less usefulness.

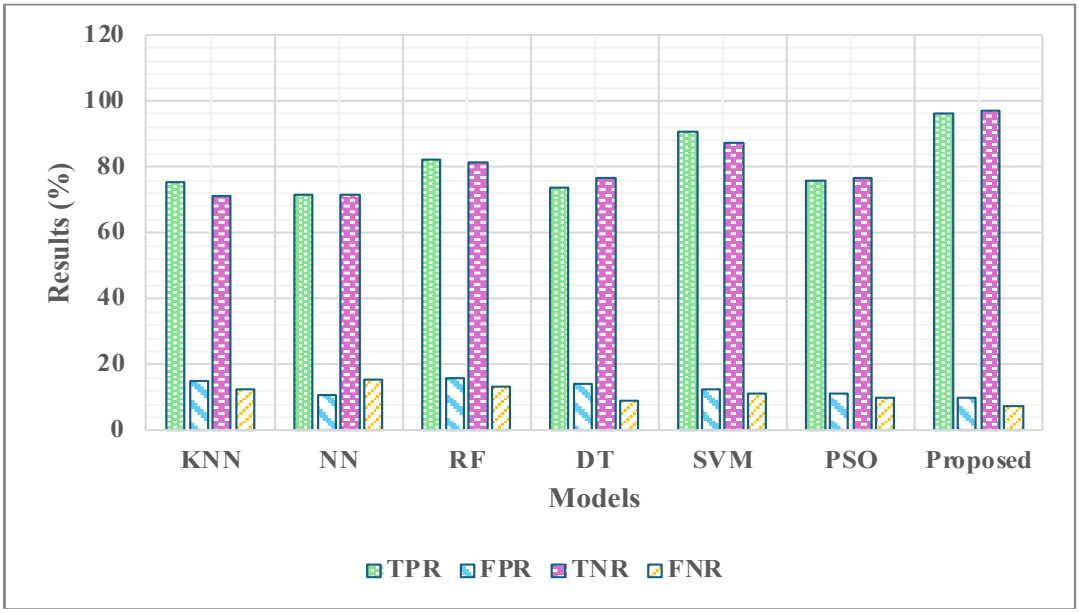

Figure 5: Confusion Matrix for NSLDD Database

The confusion matrix findings for the NSL-KDD database are shown in Figure 5. This shows how the performance of different models compares. This method has the best TPR (96.18%) and TNR (97.2%) but the worst FPR (9.85%) and FNR (7.31%). With a TPR of 90.89%, SVM does very well, but the suggested method does even better. While other models, such as RF and PSO, also get good results, they could be better than the proposed method.

5 Conclusion

This study presents a feature selection-based IDS method for IG systems. The research employed weighted PSO to enhance the FAR in the IDS. CNN and GRU are used for the classification model. Optimal characteristics are extracted from the KDD-99 and NSL-KDD databases. After selecting optimum characteristics, these characteristics are sent to ML algorithms. The research implemented many ML methods on the NSL-KDD and KDD-99 databases during the studies. Following the database gathering, the research converted them into a binary categorization: attack category and regular group, while including different attack types. Nine assaults are employed for the KDD-99 database.

In contrast, the NSKDD database employs 21 attacks. At first, the research was conducted by preprocessing the databases and substituting non-numeric variables with numerical encoding. The information is normalized by min-max normalization. The research was executed by selecting characteristics by PSO and identifying the optimal characteristics. After feature selection, the research implemented several ML techniques on both databases. RF and NN have surpassed all previous methodologies for accuracy, IDR, and FAR. Experimental findings demonstrate that the method has superior DR, FAR, and accuracy performance for the KDD-99 and NSL-KDD databases. In the future, the research wants to replicate this study across numerous classes utilizing feature selection techniques with DL techniques.

References

[1] Aljuhani, A. (2021). Machine learning approaches for combating distributed denial of service attacks in modern networking environments. *IEEE Access, 9,* 42236-42264. https://doi.org/10.1109/ACCESS.2021.3062909

[2] Anny Leema, A., Balakrishnan, P., & Jothiaruna, N. (2024). Harnessing the Power of Web Scraping and Machine Learning to Uncover Customer Empathy from Online Reviews. *Indian Journal of Information Sources and Services, 14*(3), 52–63. https://doi.org/10.51983/ijiss-2024.14.3.08

[3] Ayodeji, A., Liu, Y. K., Chao, N., & Yang, L. Q. (2020). A new perspective towards the development of robust data-driven intrusion detection for industrial control systems. *Nuclear engineering and technology, 52*(12), 2687-2698. https://doi.org/10.1016/j.net.2020.05.012

[4] Balla, A., Habaebi, M. H., Elsheikh, E. A., Islam, M. R., Suliman, F. E. M., & Mubarak, S. (2024). Enhanced CNN-LSTM deep learning for scada IDS featuring hurst parameter self-similarity. *IEEE Access, 12,* 6100 - 6116. https://doi.org/10.1109/ACCESS.2024.3350978

[5] Banumathy, D., Anitha, V., Umamaheswari, S., & Murali, T. (2023). Discharge Prediction for Critical Patients Using Machine-Learning Technology. *International Academic Journal of Science and Engineering, 10*(1), 33–38. https://doi.org/10.9756/IAJSE/V10I1/IAJSE1006

[6] Basnet, R. B., Shash, R., Johnson, C., Walgren, L., & Doleck, T. (2019). Towards Detecting and Classifying Network Intrusion Traffic Using Deep Learning Frameworks. *Journal of Internet Services and Information Security, 9*(4), 1-17. https://doi.org/10.22667/JISIS.2019.11.30.001

[7] Chaganti, R., Boppana, R. V., Ravi, V., Munir, K., Almutairi, M., Rustam, F., ... & Ashraf, I. (2022). A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. *IEEE Access, 10,* 96538-96555. https://doi.org/10.1109/ACCESS.2022.3205019

[8] D'Angelo, G., & Palmieri, F. (2021). A stacked autoencoder-based convolutional and recurrent deep neural network for detecting cyberattacks in interconnected power control systems. *International Journal of Intelligent Systems, 36*(12), 7080-7102. https://doi.org/10.1002/int.22581

[9] Fung, C. J. (2011). Collaborative Intrusion Detection Networks and Insider Attacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*(1), 63-74. https://doi.org/10.22667/JOWUA.2011.03.31.063

[10] Hasan, M. K., Habib, A. A., Islam, S., Safie, N., Abdullah, S. N. H. S., & Pandey, B. (2023). DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Reports, 9,* 1318-1326. https://doi.org/10.1016/j.egyr.2023.05.184

[11] Khan, S., Kifayat, K., Kashif Bashir, A., Gurtov, A., & Hassan, M. (2021). Intelligent intrusion detection system in smart grid using computational intelligence and machine learning. *Transactions on Emerging Telecommunications Technologies, 32*(6), e4062. https://doi.org/10.1002/ett.4062

[12] Li, X. J., Ma, M., & Sun, Y. (2023). An adaptive deep learning neural network model to enhance machine-learning-based classifiers for intrusion detection in smart grids. *Algorithms, 16*(6), 288. https://doi.org/10.3390/a16060288

[13] Liu, Q., Hagenmeyer, V., & Keller, H. B. (2021). A review of rule learning-based intrusion detection systems and their prospects in smart grids. *IEEE Access, 9,* 57542-57564. https://doi.org/10.1109/ACCESS.2021.3071263

[14] Moreno Escobar, J. J., Morales Matamoros, O., Tejeida Padilla, R., Lina Reyes, I., & Quintana Espinosa, H. (2021). A comprehensive review on smart grids: Challenges and opportunities. *Sensors, 21*(21), 6978. https://doi.org/10.3390/s21216978

Authors Biography

K. Meenakshi, received B.Tech. Information Technology from Vellore Institute of Science and Technology, Vellore in 2004 and the M.Tech. degree from the Sathyabama Institute of Science and Technology, in 2011. she has completed her Ph.D. degree in SRM Institute of Science and Technology, Kattankulathur. She is an Assistant Professor with the Department of Information Technology, SRM Institute of Science and Technology. Her research interests include Artificial Intelligence, Machine Learning, Data Mining, and Natural Language Processing. She has published 15 articles in International Journal, twenty-six articles in the Proceedings of National and International Conferences and five patents.

Dr.M. Naga Raju, is currently working as an Associate Professor in the Computer Science and Engineering Department at GITAM School of Technology GITAM (Deemed to be University) Bengaluru. His research interest is in areas such as multi-gular computing (MGc), Rough Sets, Machine Learning, and Data Science. He has published more than 18 papers in National and International Peer Review Journals and Conferences and 2 Edited Book Chapters has 2 International Patent Granted and 2 National Patents Published. He has more than 27 years of teaching experience. He wrote one book titled "Machine Learning" as a second author. He applied for one funded research project under the ISRO Respond 2023 scheme.

Dr. Channabasamma Arandi, is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Bowrampet, Hyderabad. She obtained her Ph.D. at Visvesvaraya Technological University (VTU) Belagavi in 2023. She completed her Master's degree from Acharya Institute of Technology Bangalore & BE from Poojya Doddappa Appa College of Engineering (PDACE) Gulbarga in the year 2014 and 2012 respectively. She has teaching experience of 10 years. She has 10 publications in International Conferences and reputed Journals. She is also the member of ISTE, IAENG. Her research interests include machine learning, big data analytics, NLP, and artificial intelligence.

Dr.D.V. Lalitha Parameswari, Associate Professor, Computer Science& Engineering from G. Narayanamma Institute of Technology and Science (For women), Hyderabad. She has published 20 international, scopus and SCI journals,12 conferences from various publishers and filed four patents. She has completed her M.Tech Computer Science in 2002 obtained Ph.D from JNTUH in the area of Image processing and Data Mining in 2017. She has 26 years of teaching experience. Coinvestigator for the DST Tide project with reference no. SEED/TIDE/2019/114/G and Project title: "Low-Cost Mechanism for Early Detection of Eye Diseases (Glaucoma) in Elderly" worth of Rs.37,00,410/-.

Dr.R.N. Ashlin Deepa, Associate Professor of Computer Science Engineering at Gokaraju Ranagaraju Institute of Engineering Technology has completed her doctoral degree in Computer Science Engineering from JNTU Hyderabad, India in 2021. She has over 13 years of academic experience. She obtained her M. E degree in Computer Science and Engineering from Anna University, Chennai. Her research interest includes pattern recognition, machine learning, data science, high-performance computing, etc. She has published many papers in international journals and conferences. She is also a Life Member of IEEE and ISTE. She also has published one patent to her credit. With a great passion for research, she is involved in various consultancy and research projects. She is a Principal Investigator for DST-sponsored Project in 2022.

Veena Potdar, received her B.E. degree in Computer Science in the year 1999 from Gogte Institute of Technology, Belgaum. She completed her M. Tech degree in the year 2005 from Dr. Ambedkar Institute of Technology, Bangalore & is currently working as Associate Professor in the department of Computer Science & Engineering in the same college. She has a teaching experience of 24 years. She is a permanent member of Indian Society for Technical Education, permanent member of Institute of Engineers, permanent life member of Cryptology Research Society of India & nominee member for Computer Society of India - Student chapter. Her areas of interests are cyber security, IoT & security in Databases.