Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURING SMART GRIDS WITH DEEP CNNS IN NEXT GENERATION 5G-IOT ECOSYSTEMS

B V SUBBAYAMMA[1], K S MANI[2], B SWARUPA RANI[3], MANAM RAVINDRA[4], SUDHA SREE CHEKURI[5], VASAVI MANDADI[6], BHAGYA LAKSHMI NANDIPATI[7]

[1]Department of ECE, P V P Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India

[2]Department of EEE, ACE Engineering College, Hyderabad, Telangana, India

[3]Department of EEE, Siddhartha Academy of Higher Education, Vijayawada, Andhra Pradesh, India

[4]Department of EEE, Aditya University, Surampalem, Andhra Pradedh, India

[5]Department of Computer Science and Engineering, RVR & JC College of Engineering, Guntur, India

[6]Department of Computer Science and Engineering, RVR & JC College of Engineering, Guntur, India

[7]Department of Computer Science and Engineering, RVR & JC College of Engineering, Guntur, India

E-mail: kolla.samyuktha@gmail.com, drsmanik21@gmail.com, swarupabondalapti@gmail.com, ravieeejntu@gmail.com, chekuri.sudha@gmail.com, vasavilahari@gmail.com, bhagyalakshmi.nandipati@gmail.com

ABSTRACT

The implementation of 5G networks and IoT devices in smart grid applications facilitates the electricity-generated, distributed, and managed bidirectional transfer of real-time information between utility suppliers and consumers. Nonetheless, this heightened transmission and assurance in IoT devices also introduce unprecedented security issues, as they are susceptible to malicious assaults. Implementing effective attack detection techniques in 5G-IoT smart grid systems for dependable and efficient power distribution, together with the prompt and precise identification of attacks, is essential. A novel technique, termed Target Projection Regressed Gradient Convolutional Neural Network (TPRGCNN), is developed to enhance the accuracy of attack detection in data transmission inside a 5G-IoT smart grid context. The TPRGCNN approach integrates feature selection and classification to enhance secure data transfer by identifying assaults in 5G-IoT smart grid networks. During the feature selection process, TPRGCNN employs the Ruzicka coefficient Dichotonic projection regression approach to improve attack detection accuracy while reducing time complexity. Subsequently, the chosen significant features are input into Jaspen's correlative stochastic gradient convolutional neural learning classifier for the purpose of attack detection. Classification determines if the transmission is standard or indicative of an assault within the 5G-IoT smart grid network. The implementation findings indicate that the suggested TPRGCNN approach achieves a 5% enhancement in attack detection accuracy and a 2% increase in precision, recall, and F-score, while simultaneously reducing time complexity and space complexity by 13% and 23%, respectively, in comparison to existing methods.

Keywords: *5G-Iotattack Detection, Smart Grid, Ruzicka Coefficient, Convolutional Neural Classifier, Soft Step Activation*

1. INTRODUCTION

The integration of 5G technology in smart grids facilitates enhanced communication capabilities, allowing for innovative monitoring and control tactics. This enables collaborative communication between utility providers and users, facilitating effective management of electricity usage. Smart grid devices necessitate bidirectional connectivity to routinely exchange information in order to perform these activities. Securing these connections is essential for augmenting the overall security of smart grid entities. The integration of 5G-IoT within the smart grid requires the adoption of stringent security measures to identify and alleviate possible threats. It is essential to address emerging attack vectors and vulnerabilities resulting from the confluence of 5G and IoT

Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

technologies within the smart grid. Figure 1 illustrates the assaults occurring in the generating, transmission, and distribution sectors within a smart grid context. Cyber-attacks can target power plants, jeopardizing its control systems, resulting in interruptions in electricity generation or even physical damage to essential components. Hackers can exploit communication networks or data flow during transmission, resulting in grid instability or unauthorized power rerouting. Moreover, in the distribution sector, vulnerabilities in smart meters or sensors may be used to manipulate consumption data or interrupt service to end-users. These assaults jeopardize the operational integrity of the grid and elevate concerns regarding data privacy and the risk of extensive blackouts, underscoring the imperative for stringent cybersecurity protocols and ongoing surveillance to protect against such threats.

A hybrid deep learning system was developed in [1] to identify Distributed Denial of Service threats on the communication network of the Smart Grid. The suggested Hybrid method comprised a combination of Convolutional Neural Networks and Gated Recurrent Units. Nonetheless, the performance of the network intrusion detection system did not meet expectations. A Bayesian method integrated with deep convolutional neural networks (CNN-Bayesian) was established in [2] to differentiate cyber-physical intrusions from regular occurrences by managing a high-dimensional feature space. Nonetheless, it failed to concentrate on the implementation of the distributed machine learning framework combined with Bayesian techniques to enhance the efficacy of classification algorithms.

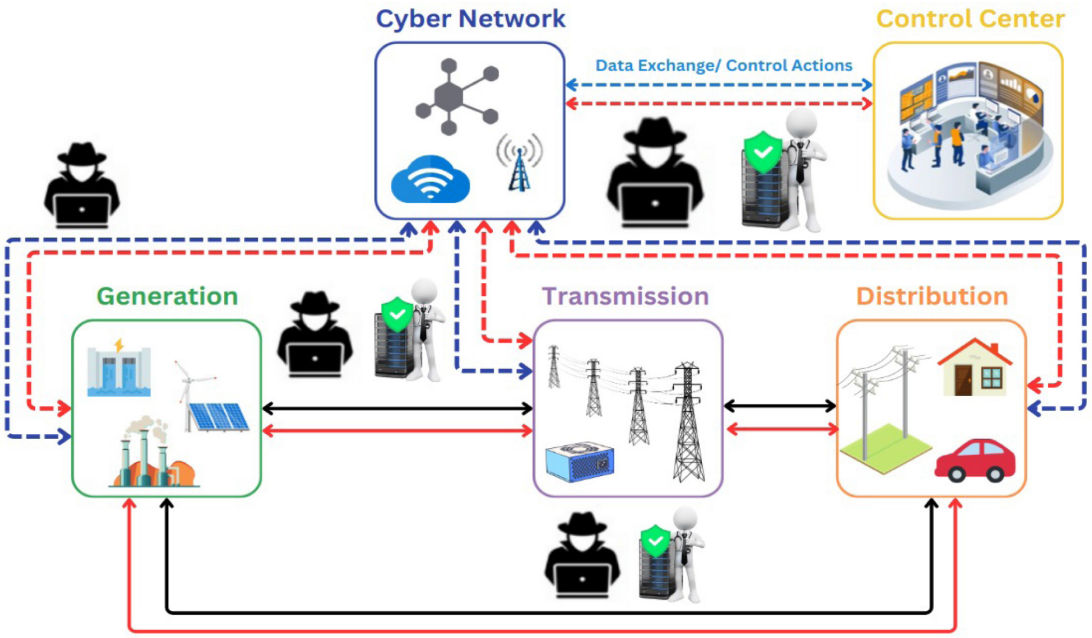

Figure 1: Assaults in Smart Grid Context

We created a supervised machine learning technique [3] to detect intrusions in a smart grid scenario by extracting a collection of features. This was done in order to identify potential threats. Nevertheless, it did not take into account multilabel categorization, which is designed to not only determine whether or not the smart grid is being attacked, but also to determine the type of attack that is currently being carried out over it. In order to develop a unique intrusion detection system for smart grids, the merging of deep learning and feature selection approaches is utilized in [4]. On the other hand, it did not implement any further advanced machine learning techniques, such as convolution neural networks (CNNs), in order to enhance the effectiveness of intrusion detection.

The bilinear map pairing-based authentication technique that was presented in [5] has the specific objective of enhancing the safety of the smart grid and identifying any potential assaults that may

occur. However, because it incorporates more security elements, it comes with increased calculation costs. This is a consequence of the process. In order to identify the fake data injection attack that was being carried out in the smart grid, the stacked autoencoder approach was created [6]. Nevertheless, the method that was created was not successful in detecting cyber attacks on systems.

For the purpose of intrusion detection, a Convolutional Neural Network (CNN) architecture was created with reference to [7]. Despite this, it did not contribute to an improvement in performance, particularly with regard to the classification of various types of intrusions. For the purpose of improving the safety of Internet of Things (IoT)-based smart devices, machine learning techniques were created [8]. On the other hand, the time complexity of the algorithms that were devised was not minimized. An innovative approach that is based on deep learning was developed in [9] with the purpose of improving the accuracy of cyber threat identification. The system, on the other hand, was not able to reliably identify both internal and external intruders in real time during the validation process.

[10] was the year that a Blockchain-Assisted Data Edge Verification with Consensus Algorithm was developed for the aim of Internet of Things defect detection in order to improve security. Significant feature selection, on the other hand, was a major cause for concern. The resource restrictions of devices in recognizing malware attacks in 5G Internet of Things smart grids lay in the need for personalized, flexible, real-time, and privacy-preserving detection approaches that answer the special problems faced by this dynamic and complex ecosystem. These methods must be able to recognize malware attacks simultaneously. A significant amount of progress has been made in increasing the resilience of smart grids and Internet of Things networks against cyber threats, which will ultimately contribute to the creation of digital infrastructure that is safer and more secure.

2. RELATED WORKS

Figures should be labeled with "Figure" and tables with "Table" and should be numbered sequentially, for example, Figure 1, Figure 2 and so on (refer to table 1 and figure 1). The figure numbers and titles should be placed below the figures, and the table numbers and titles should be placed on top of the tables. The title should be placed in the middle of the page between the left and right margins. Tables, illustrations and the corresponding text should be placed on the same page as far as possible if too large they can be placed in singly column format after text. Otherwise they may be placed on the immediate following page. If its size should be smaller than the type area they can be placed after references in singly column format and referenced in text

An artificial intelligence (AI)-based attack-detection and prevention (ADP) method was designed [11] by applying a cryptography-driven recommender system to guarantee data security. However, the system failed to improve attack detection with higher accuracy. An integrated framework was designed in [12] with the aim of Intrusion Detection for smart grids which combines feature engineering-based preprocessing with machine learning classifiers. A novel intelligent and autonomous deep-learning model was designed [13] for the detection and classification of cyber-attacks in IoT communication networks. But designed model failed to minimize computation complexity.

A deep learning-based state forecasting model was developed in [14] for false data injection detection using the error covariance matrix. However, the approach designed for implementing the smart grid did not meet the stricter detection benchmark, resulting in a higher probability of identifying injection attacks. A hybrid machine learning approach was introduced [15] for enhancing DDoS attack detection in smart grid applications and cyber security. However, the deep feature analysis was not performed to improve the accuracy of attack detection. A correlation approach called Detection of Multi-Stage Coordinated Attacks (DOMCA) was designed [16] to identify suitable attacks. However, decision support systems and automated responses to cyber attacks remained unaddressed.

A whale optimization algorithm (WOA)-trained Artificial Neural Network (ANN) was designed in [17] for intrusion detection. The weight vector of ANN was adjusted during training in order to minimize error. An optimal feature selection-based intrusion detection system was introduced in [18] for smart grid systems. However, the consideration of multiple classes with feature selection methods using deep learning algorithms was not included.

A divergence-based transfer ability analysis was designed in [19] for intrusion detection with a transfer learning approach. However, it failed to evaluate more advanced coordinated attack scenarios to verify performance and improve the

transfer ability analysis. A deep learning model was developed in [20] for anomaly detection and classification to detect TCP cyberattacks. However, it failed to include the execution of other deep learning models in order to detect cyberattacks with higher accuracy.

A novel Software Defined Networks (SDN)-based smart grid (SG) architecture was introduced in [21] with improved security by deployment of a distributed. However, failed to perform the novel security with this designed method. An intelligent intrusion detection system for a smart grid was implemented in [22] with utilization of image processing and analysis, but the network traffic does not have animage-type nature. Moreover, the significant challenge in providing an ID system for SG network is that traffic imbalance reduces the ability to detect attacks with deep learning methods. In [23], a fog-edge-enabled Support Vector Machine (SVM)-based federated learning(FL) IDS for SG was designed. The designed method was not focus on time and space complexity.

In [24], a feasibility of using cloud solutions to support federated learning-based anomaly detection in smart grids were investigated into improve the connectivity and enhance the security. However, the specificity was not considered to the designed method. A comprehensive network-slicing model was combined in [25] with an attack detection system within the 5G framework. However, the accuracy was not improved by designed model. A novel industry architecture was introduced in [26] to identify and analyze the potential technical connectivity architectures and industry architectures necessary in providing connectivity solutions for the smart distribution grids.

A monitoring method of stealthy complex network attacks were designed in [27] to considering the security situation awareness. However, the monitoring nodes of stealth complex network attacks are effectively minimizing the resource occupancy rate of monitoring nodes and enhance the monitoring accuracy. In [28], a comprehensive overview of SG technology performed into highlighting the current state of SG implementation by a variety of industrial, governmental, and academic institutions. A smart grid using big data and AI were introduced in [29] to vital the improved energy needs of our society when promoting sustainability and minimum greenhouse gas emissions. However, their security remains a significant challenge. A Network and cyber security applications of defense in adversarial attacks were investigated in [30] to attacks from opponents described on adversarial attacks. The designed method was improving the cyber security and also space complexity was not focused. With development of communication networks, computational units, and control systems, cyber–physical power systems (CPPSs) [31], [32] remained difficult task. In smart systems, a large amount of data is generated, exchanged and processed for different purposes. With the strong interactions, CPPSs employed different security vulnerabilities. For performing the security operation and control of CPPSs, it is required to identify the locations of attacked measurements and removed the state bias caused by malicious cyber-attacks like false data inject attack, jamming attack, denial of service attack, or hybrid attack.

3. PROPOSAL METHODOLOGY

As a technologically enhanced power grid paradigm, the smart grid has garnered a solid reputation in recent years. It is a sophisticated cyber–physical system that integrates Internet of Things technology with grid infrastructure in order to make it possible to control operations remotely. One of its most important characteristics is the incorporation of smart meters, which can facilitate the exchange of data in real time between users and energy companies. On the other hand, the broad implementation of smart grids has resulted in a high number of issues regarding privacy and security. Among these are the fact that it is possible for unauthorized individuals to access sensitive data and the capability to change data. Not only is it essential to immediately and properly detect any security vulnerabilities that may occur in the system, but it is also essential to ensure that the power distribution system is both reliable and efficient while also protecting against such threats. The provision of a secure service in smart grid systems is made possible by intrusion detection, which simultaneously notifies the system in a timely manner of any adversary attacks that have been identified. In this paper, an intelligent intrusion detection strategy that is proposed and given the name TPRGCNN is presented. The purpose of this scheme is to accurately categorize the many different kinds of attacks that can be made against smart power grid systems. A representation of the architecture diagram of the TPRGCNN technique that has been suggested can be found in Figure 2. This technique is comprised of two primary processes: feature selection and classification. The purpose of this project is to improve the accuracy of attack detection in a 5G-

Internet of Things smart grid network while data is being transmitted. A device connected to the internet of things is initially installed in a smart grid field for the purpose of monitoring and carrying out remote control data transfer. The NSL-KDD network dataset, which is a network intrusion detection dataset, is utilized in the beginning of the TPRGCNN technique, which is a feature selection procedure from the beginning. For the purpose of analyzing feature sets and projecting relevant features, the Ruzicka coefficient Dichotonic projection regression technique is utilized. The dataset is then cleaned of features that are redundant with one another. Following the selection of relevant features, the TPRGCNN approach moves on to the classification phase in order to detect attacks. For the purpose of identifying threats in a 5G-Internet of Things smart grid network, the correlative stochastic gradient convolutional neural learning classifier developed by Jaspen is applied. Each of these two procedures of the TPRGCNN technique that has been presented will be discussed in the following subsections in its own right.

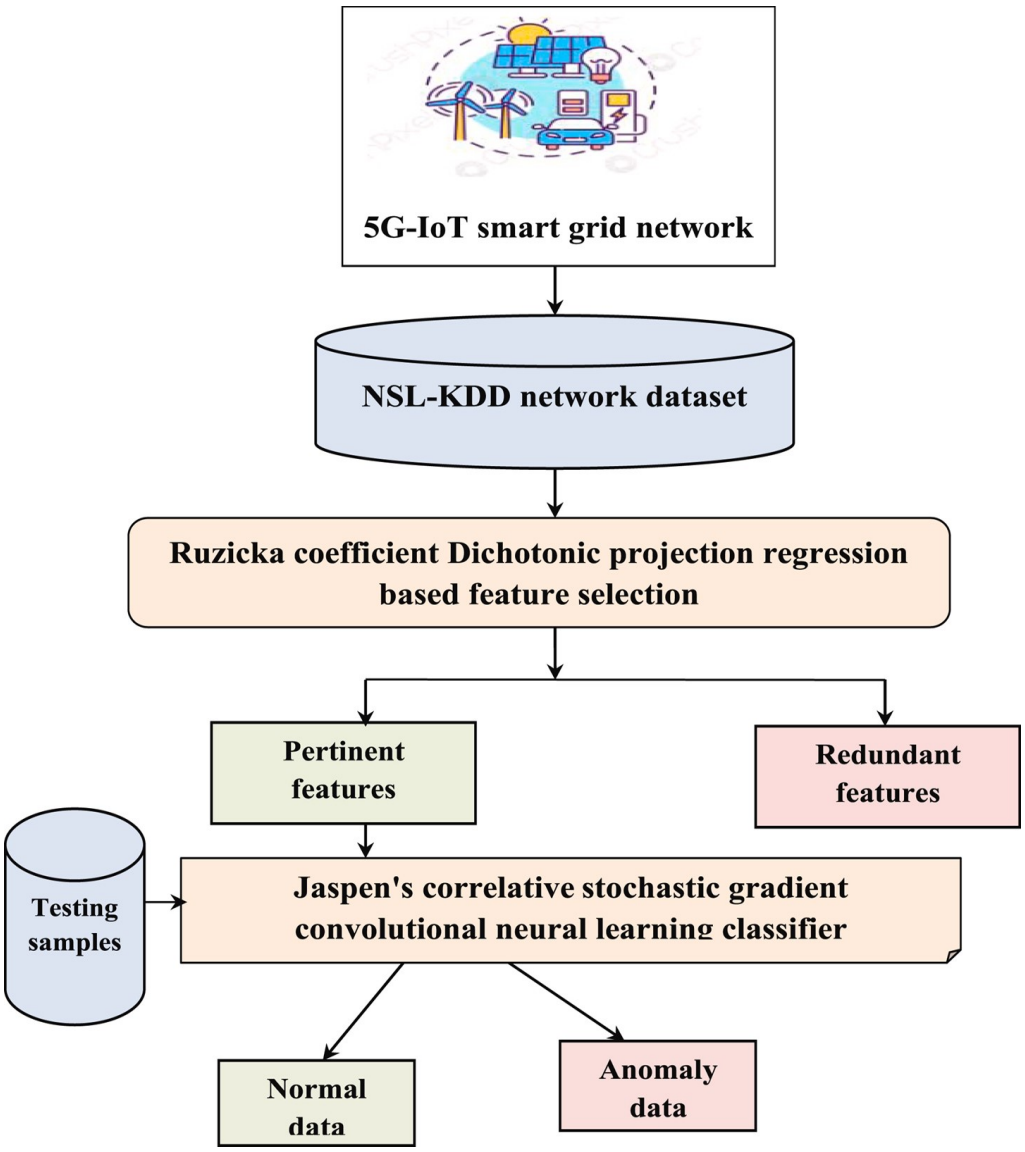

Figure 2: Structure of TPRGCNN

Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

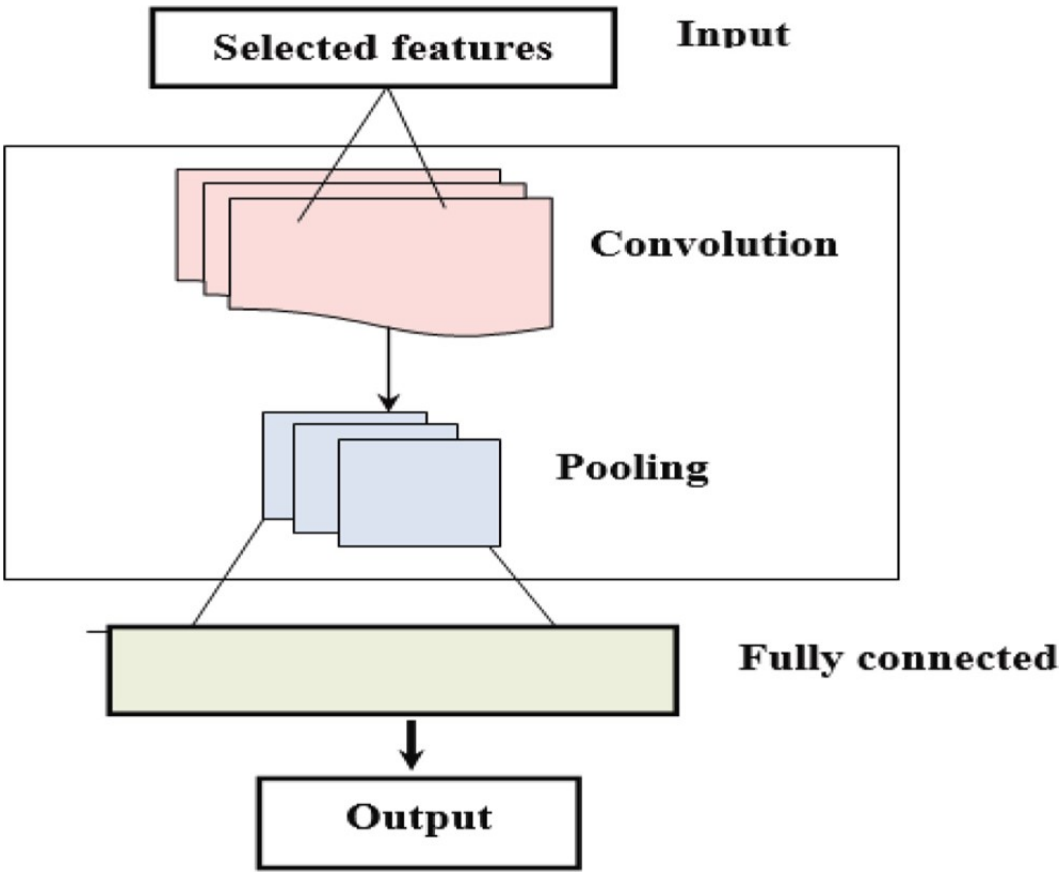

Figure 3: Structure of the convolutional neural network

The initial step of the proposed TPRGCNN method involves selecting features to identify a subset of pertinent characteristics from a broader array of available features in a dataset for the purpose of attack detection. This represents a crucial advancement in the fields of machine learning and data analysis, as it contributes to improving model performance while simultaneously decreasing time complexity. The primary objective of feature selection is to identify the most informative and distinguishing features. The process of feature selection improves the model's capability for attack detection in smart grid applications by removing irrelevant or redundant features. The proposed TPRGCNN technique employs Ruzicka coefficient Dichotonic projection regression. A regression is a statistical method employed to assess the relationship between variables in the dataset through the application of a Ruzicka coefficient. Dichotonic refers to the division of features into two equal categories: pertinent and redundant.

Figure 3 depicts the architecture of a convolutional neural network. The convolutional neural network consisted of input, output, and three types of hidden layers: convolution, pooling, and fully connected, as outlined in the proposed TPRGCNN technique. The architecture accepts the chosen subset of features along with the data samples as a training set at the input layer. The selected features undergo processing in the convolutional, pooling, and fully connected layers. The result is ultimately presented at an output layer. The convolutional layer serves as the fundamental element of the architecture, applying a specific set of weights to the input data. Each weight convolves with the input, executing element-wise multiplications and aggregating the outcomes.

It is common practice for an architecture to incorporate pooling layers in addition to convolutional layers. These layers are responsible for down sampling feature maps that are generated by convolutional layers. A reduction in spatial dimensions can be achieved through pooling, while

the most significant results are maintained. The pooling process that is utilized the most frequently is known as max pooling. This allows for the selection of the maximum value, which is the positive correlation between two data instances. The occurrences that have unfavorable relationships with one another are disregarded.

It is common practice to send the output of the correlation layer to fully connected layers after it has been passed through numerous convolutional and pooling layers. Because of the correlation results obtained from the feature map, these layers are responsible for performing high-level reasoning and categorization.

Regular neural networks and fully connected neural networks share a property in which each neuron in the fully connected layer is connected to all of the activations that occurred in the layer below it. For the purpose of providing final output classification results, the soft step activation function is applied in a fully connected layer. The input values for the classification are positive correlation coefficient parameters.

4. RESULTS AND DISCUSSION

This section presents the evaluation of the TPRGCNN method alongside existing hybrid deep learning algorithms [1] and CNN-Bayesian [2], implemented in Python utilizing the NSL-KDD dataset. The dataset is sourced from [33] to analyze network attacks occurring during data transmission in the 5G-IoT smart grid network. The KDDTrain+.arff folder is sourced from the dataset for the purpose of conducting the simulation. The dataset includes 125,973 instances for both training and testing data. The dataset comprises 42 features related to smart grid flow, including several notable examples. Relevant features are selected from the total number of features to execute the attack detection. The NSL-KDD dataset in the training set comprises only relevant data. The test set contains no duplicate data. The quantity of data selected from each complexity level in the new KDD dataset is specified. Machine learning methods are employed for classification to achieve accurate estimations. The quantity of instances serves as a metric for evaluating experiments within training and testing datasets to enhance performance. In each iteration, samples of 10,000, 20,000, 30,000, up to 100,000 are extracted from the dataset.

The results section outlines the findings obtained from a series of controlled experiments designed to evaluate the performance and efficiency of the proposed TPRGCNN method. The primary aim of these experiments was to evaluate the influence of results or performance metrics for an in-depth analysis of the model across various conditions. This section presents an analysis of various results, including ROC, AUC, and specificity, derived from the proposed TPRGCNN method alongside existing hybrid deep learning algorithms [1] and CNN-Bayesian [2].

Figure 4 presents the experimental outcomes regarding the specificity of three methodologies: the proposed TPRGCNN method, an existing hybrid deep learning algorithm [1], and CNN-Bayesian [2]. The specificity is quantified by the true negative samples and the total of true negative and false positive samples, which plays a crucial role in enhancing 5G networks for smart grid applications through attack detection. The specificity is improved through the application of the TPRGCNN method in comparison to the existing methods [1], [2].

Figure 5 illustrates that an increase in the false-positive rate led to an enhancement in the true positive rate of the proposed TPRGCNN method. A higher AUC score indicates improved performance of the classifier. This suggests that the proposed TPRGCNN method demonstrates improved accuracy with an increase in the number of samples.

A graphical representation of the accuracy of attack detection is shown in Figure 6, which plots the accuracy versus the number of cases chosen from the dataset. The axis displays the overall accuracy results, while the axis displays the number of cases that were found to be accurate. TPRGCNN achieves a greater level of accuracy in attack detection when compared to other hybrid deep learning algorithms [1] and CNN-Bayesian [2]. This is demonstrated by the graph. As a result of the deployment of Jaspen's correlative stochastic gradient convolutional neural classifier, this enhancement has been stored. Through the utilization of Jaspen's correlation function, the deep learning model that has been provided is able to successfully assess both training and testing examples. When highly correlated outcomes are identified, the correlation measure is utilized to identify them. These results are then analyzed with the help of the soft step activation function. Lastly, the output layer is responsible for classifying instances as either normal or anomalous, which ultimately results in greater accuracy in attack detection.

Journal of Theoretical and Applied Information Technology
30th June 2025. Vol.103. No.12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

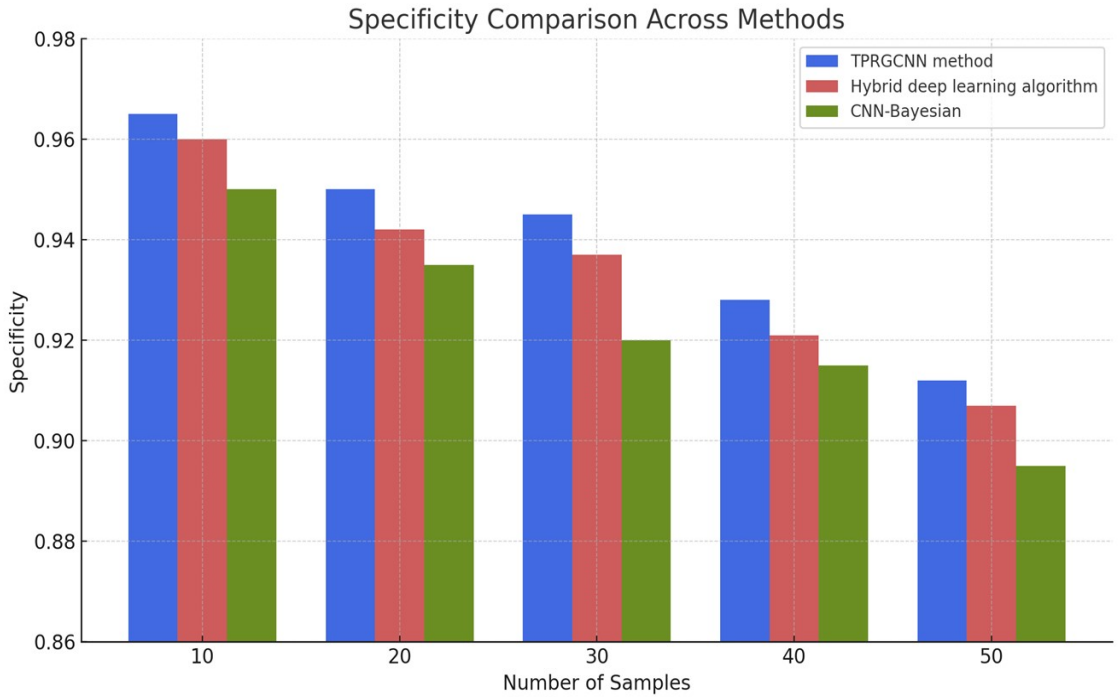

Figure 4: Relationship between specificity and sample size

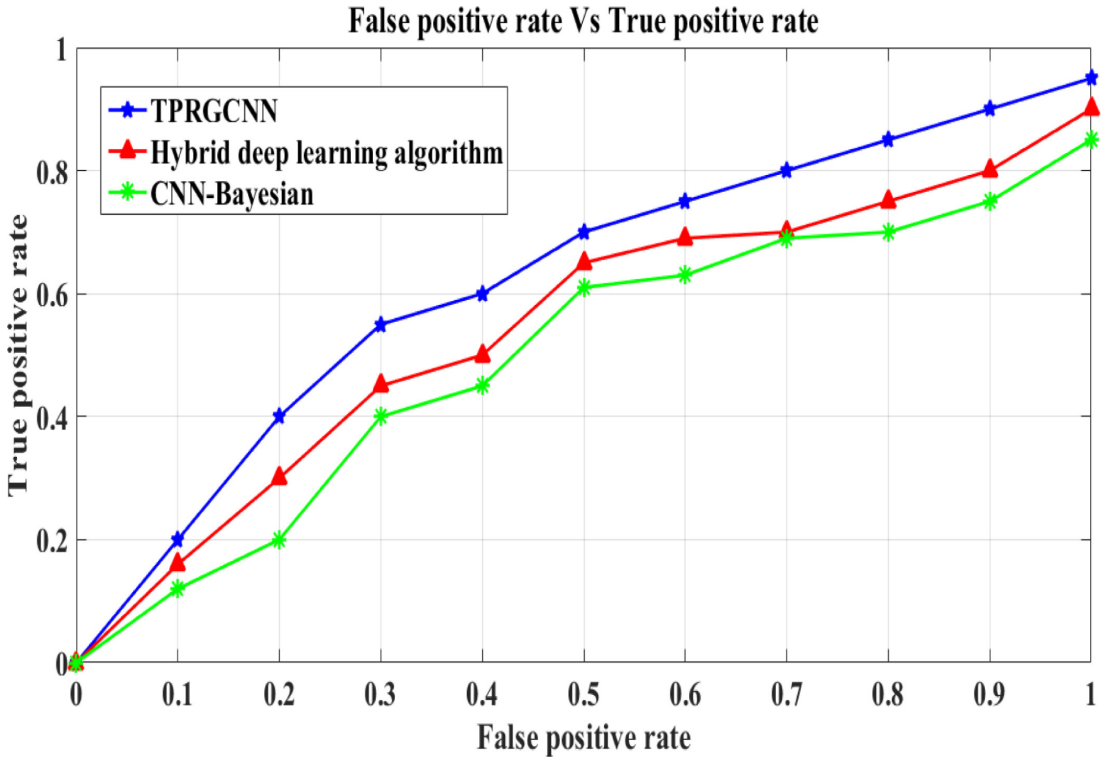

Figure 5: The AUC value associated with the ROC curve for the proposed TPRGCNN method.

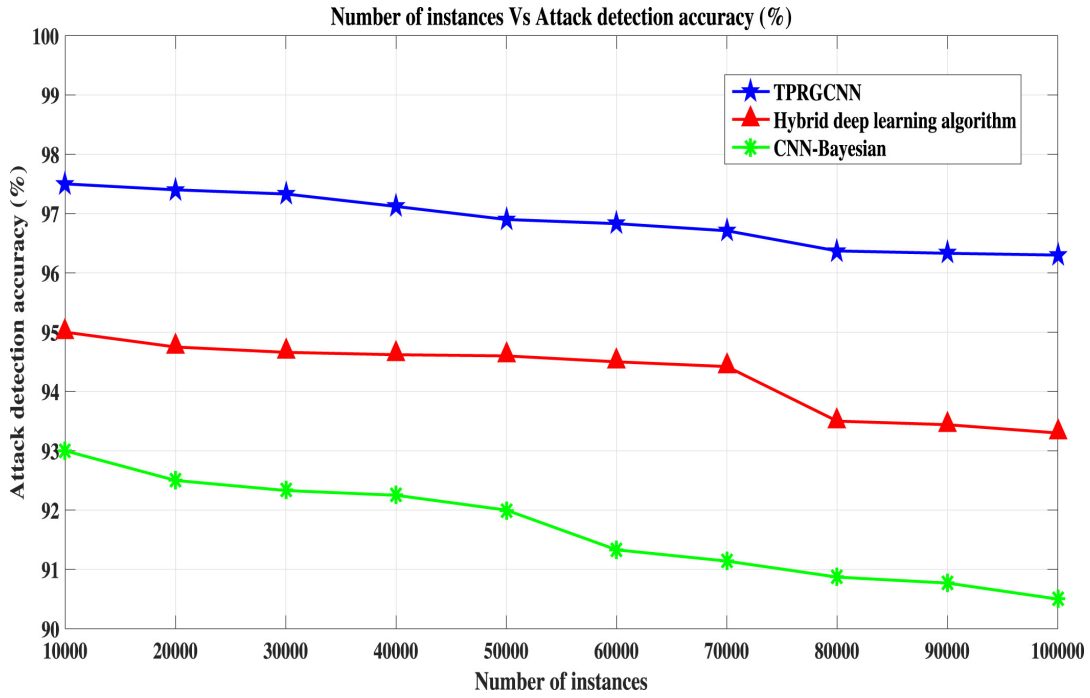

Figure 6. Instances compared to accuracy in attack detection

5. CONCLUSION

This work presents a technology named TPRGCNN, designed to improve the dependability of the smart grid by promptly identifying and differentiating suspicious and abnormal events. Cybersecurity poses a critical challenge for smart grid systems because of their reliance on cyberinfrastructure, which manages and disseminates substantial volumes of data produced during operational processes. The TPRGCNN method initiates by identifying pertinent features from the network attack detection dataset. Subsequently, Jaspen's correlative stochastic gradient convolutional neural network classifier is utilized to assess training and testing data for identifying typical or aberrant behavior. The stochastic gradient descent algorithm is employed to reduce errors in attack detection. To assess the efficacy of the TPRGCNN technique, simulations are performed utilizing several criteria, such as attack detection accuracy, precision, recall, F-score, and time complexity. The implementation findings indicate that the suggested TPRGCNN approach achieves a 5% enhancement in attack detection accuracy and a 2% increase in precision, recall, and F-score, while simultaneously reducing time complexity and space complexity by 13% and 23%, respectively, in comparison to existing methods.

REFERENCES:

[1] S.Y. SDiaba, M. Elmusrati, Proposed algorithm for smart grid ddos detectionbased on deep learning, Neural Netw. 159 (2023) 175–184,http://dx.doi.org/10.1016/j.neunet.2022.12.011.

[2] D. Kaur, et al., A bayesian deep learning approach with convolutional featureengineering to discriminate cyber–physical intrusions in smart grid systems,IEEE Access 11 (2023) 18910–18920,http://dx.doi.org/10.1109/access.2023.3247947.

[3] F. Martinelli, F. Mercaldo, A. Santone, A method for intrusion detection in smartgrid, Procedia Comput. Sci. 207 (2022) 327–334,http://dx.doi.org/10.1016/j.procs.2022.09.066.

[4] C. Song, et al., Intrusion detection based on hybrid classifiers for smart grid,Comput. Amp Electr. Eng. 93 (2021) 107212,http://dx.doi.org/10.1016/j.compeleceng.2021.107212.

[5] Y. Chen, et al., A bilinear map pairing based authentication scheme for smartgrid communications: Pauth, IEEE Access 7 (2019) 22633–

22643,http://dx.doi.org/10.1109/access.2019.2898376.

[6] L. Chen, et al., Stacked autoencoder framework of false data injection attackdetection in smart grid, Math. Probl. Eng. 2021 (2021) 1–8,http://dx.doi.org/10.1155/2021/2014345.

[7] O.D. Okey, et al., Transfer learning approach to ids on cloud IOT devices usingoptimized CNN, IEEE Access 11 (2023) 1023–1038,http://dx.doi.org/10.1109/access.2022.3233775.

[8] M.S. Abdalzaher, et al., Toward secured IOT-based smart systems using ma-chine learning, IEEE Access 11 (2023) 20827–20841,http://dx.doi.org/10.1109/access.2023.3250235.

[9] I.A. Kandhro, et al., Detection of real-time malicious intrusions and attacks inIOT empowered cybersecurity infrastructures, IEEE Access 11 (2023) 9136–9148,http://dx.doi.org/10.1109/access.2023.3238664.

[10] T. Vaiyapuri, et al., Blockchain assisted data edge verification with consensus al-gorithm for machine learning assisted IOT, IEEE Access 11 (2023) 55370–55379,http://dx.doi.org/10.1109/access.2023.3280798.

[11] A. Kumari, et al., Ai-empowered attack detection and prevention scheme forsmart grid system, Mathematics 10 (16) (2022) 2852,http://dx.doi.org/10.3390/math10162852.

[12] D. Upadhyay, et al., Gradient boosting feature selection with machine learningclassifiers for intrusion detection on power grids, IEEE Trans. Netw. Serv. Manag.18 (1) (2021) 1104–1116,http://dx.doi.org/10.1109/tnsm.2020.3032618.

[13] Q. Abu Al-Haija, S. Zein-Sabatto, An efficient deep-learning-based detectionand classification system for cyber-attacks in IOT communication networks,Electronics 9 (12) (2020) 2152,http://dx.doi.org/10.3390/electronics9122152.

[14] D. Mukherjee, et al., Deep learning-based identification of false data injectionattacks on modern smart grids, Energy Rep. 8 (2022) 919–930,http://dx.doi.org/10.1016/j.egyr.2022.10.270.

[15] M.K. Hasan, et al., DDoS: Distributed denial of service attack in communicationstandard vulnerabilities in smart grid applications and cyber security with recentdevelopments, Energy Rep. 9 (2023) 1318–1326,http://dx.doi.org/10.1016/j.egyr.2023.05.184.

[16] Ö. Sen, et al., On using contextual correlation to detect multi-stage cyberattacks in smart grids, Sustain. Energy Grids Netw. 32 (2022) 100821,http://dx.doi.org/10.1016/j.segan.2022.100821.

[17] L. Haghnegahdar, Y. Wang, A whale optimization algorithm-trained artificialneural network for smart grid cyber intrusion detection, Neural Comput. Appl.32 (13) (2019) 9427–9441,http://dx.doi.org/10.1007/s00521-019-04453-w.

[18] S. Khan, et al., Intelligent intrusion detection system in smart grid usingcomputational intelligence and machine learning, Trans. Emerg. Telecommun.Technol. 32 (6) (2020) 00,http://dx.doi.org/10.1002/ett.4062.

[19] P. Liao, et al., Divergence-based transferability analysis for self-adaptivesmart grid intrusion detection with transfer learning, IEEE Access 10 (2022)68807–68818,http://dx.doi.org/10.1109/access.2022.3186328.

[20] I. Siniosoglou, et al., A unified deep learning anomaly detection and classificationapproach for smart grid environments, IEEE Trans. Netw. Serv. Manag. 18 (2)(2021) 1137–1151,http://dx.doi.org/10.1109/tnsm.2021.3078381.

[21] S. Chatzimiltis, M. Shojafar, M.B. Mashhadi, R. Tafazolli, A collaborative softwaredefined network-based smart grid intrusion detection system, IEEE Open J.Commun. Soc. 5 (2024) 700–711,http://dx.doi.org/10.1109/OJCOMS.2024.3351088.

[22] Ahmed AbdulmunemMhmood, Özgür Ergül, Javad Rahebi, Detection of cyber-attacks on smart grids using improved VGG19 deep neural network architectureand aquila optimizer algorithm, SIViP 18 (2024) 1477–1491,http://dx.doi.org/10.1007/s11760-023-02813-7.

[23] Noshina Tariq, Amjad Alsirhani, Mamoona Humayun, FaeizAlserhani and mom-ina shaheen. a fog-edge-enabled intrusion detection system for smart grids, J.Cloud Comput. 13 (2024) 43,http://dx.doi.org/10.1186/s13677-024-00609-9.

[24] J. Jithish, Nagarajan Mahalingam, Yeo Kiat Seng, Empowering smart gridsecurity: Towards federated learning in 6G-enabled smart grids using

cloud,2024,http://dx.doi.org/10.21203/rs.3.rs-3834382/v1.

[25] Abood, Mohammed Salah, Hua Wang, Bal S. Virdee, Dongxuan He, Maha Fathy,Abdulganiyu Abdu Yusuf, Omar Jamal, et al., Improved 5G network slicingfor enhanced QoS against attack in SDN environment using deep learning, IETCommun. 18 (13) (2024) 759–777,http://dx.doi.org/10.1049/cmu2.12735.

[26] S. Borenius, P. Kekolahti, H. Hämmäinen, M. Lehtonen, P. Mähönen, Novelindustry architectures for connectivity solutions in the smart distribution grids,IEEE Access 11 (2023) 68093–68112,http://dx.doi.org/10.1109/ACCESS.2023.3291745.

[27] Xi, Bo, Huiying Liu, Botao Hou, Ying Wang, Yuling Guo, Stealing complexnetwork attack detection method considering security situation awareness, PlosOne 19 (3) (2024) e0298555,http://dx.doi.org/10.1371/journal.pone.0298555.

[28] J. Powell, A. McCafferty-Leroux, W. Hilal, S.A. Gadsden, Smart grids: A com-prehensive survey of challenges, industry applications, and future trends, EnergyRep. 11, 5760–5785,http://dx.doi.org/10.1016/j.egyr.2024.05.051.

[29] Ghadi, Yazeed Yasin, Tehseen Mazhar, Khursheed Aurangzeb, Inayatul Haq,Tariq Shahzad, Asif Ali Laghari, Muhammad Shahid Anwar, Security risk modelsagainst attacks in smart grid using big data and artificial intelligence, PeerJComput. Sci. 10 (2024) e1840,http://dx.doi.org/10.7717/peerj-cs.1840.

[30] Yahya Layth Khaleel, Mustafa Abdulfattah Habeeb, A.S. Albahri, Tahsien Al-Quraishi, O.S. Albahri, A.H. Alamoodi, Network and cybersecurity applicationsof defense in adversarial attacks: A state-of-the-art using machine learning anddeep learning methods, J. Intell. Syst. 33 (1) (2024) 20240153,http://dx.doi.org/10.1515/jisys-2024-0153.

[31] K.-D. Lu, L. Zhou, Z.-G. Wu, Representation-learning-based CNN for intelligentattack localization and recovery of cyber-physical power systems, IEEE Trans.Neural Netw. Learn. Syst. 35 (5) (2024) 6145–6155,http://dx.doi.org/10.1109/TNNLS.2023.3257225.

[32] K.-D. Lu, Z.-G. Wu, T. Huang, Differential evolution-based three stage dynamiccyber-attack of cyber-physical power systems, IEEE/ASME Trans. Mechatronics28 (2) (2023) 1137–1148,http://dx.doi.org/10.1109/TMECH.2022.3214314.

[33] Hassan06, NSL-KDD Dataset, Kaggle, 2020, Availablehttps://www.kaggle.com/datasets/hassan06/nslkdd.