Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549839

CLASSIFICATION OF INTRUSION IN SMART POWER GRID SYSTEM USING SVM WITH PREPROCESSING APPROACHES

T.Jenish
Research Scholar, Department of Electronics and Communication Engineering, Dr.M.G.R
Educational and Research Institute, Maduravoyal, Chennai – 95, India

M.Kumaresan
Professor, Department of Electronics and Communication Engineering, Dr.M.G.R
Educational and Research Institute, Maduravoyal, Chennai – 95, India

Y.Candida
Assistant Professor, Department of Electronics and Communication Engineering, Dr.M.G.R
Educational and Research Institute, Maduravoyal, Chennai – 95, India

Abstract: - The security and dependability of smart power grids are crucially dependent on intrusion detection. Smart grids' use of modern communication and technological advances opens up new security gaps and areas for attack. IDS (Intrusion Detection Systems) is created to watch over and examine network traffic to spot any suspicious or fraudulent activity that might point to unauthorized access or possible cyber threats. By using data pretreatment approaches such as SMOTE for dealing with imbalanced datasets, z-score or MinMax scaling for feature normalization and PCA for dimensionality reduction, this study suggests an intrusion detection framework for smart power grids. The Support Vector Machine (SVM) algorithm is used to perform the classification problem. The framework intends to improve the precision and effectiveness of intrusion detection in smart power grids while also offering a strong defense against online attacks and guaranteeing the infrastructure's safety and dependability.

Keywords: - Intrusion Detection, Classification, Threats, Attacks, System

I INTRODUCTION

The size of the Internet is expanding, information volume is exploding in the information age and network security is becoming more and more crucial. A crucial tool for ensuring the security of the network environment, intrusion detection is recognized as a classic security protection technology [1]. It's critical to lessen the vulnerabilities in Smart Grid Technology because cyber security is a growing area of concern [2]. Today's smart grid network includes a wide range of middleware components, including electrical equipment that spins or vibrates databases, storage, caches, and identification services, among others. Every element is a separate collection of real or simulated computers that together provide a significant amount of data in the form of logs and metrics. If any of these high-vibrating machines fails, the system is going to shut down completely. As an outcome, the smart grid equipment's condition surveillance system is more reliable and effective at anticipating the machine's condition. It takes longer to evaluate data provided by every element and requires more processing abilities to analyze the data and draw any conclusions for further analysis and anomaly detection [3]. Following Fig 1 describes the basic structure of the smart grid.

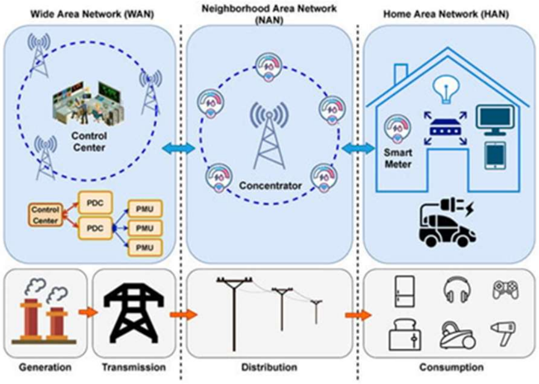

Fig 1 Smart Grid Structure [22]

Due to the increasingly intricate coordination of many system components, their rise poses significant operational issues for the power system. As a result, the cyber-layer incorporates more effective control strategies. The operation of the energy layer is monitored, protected, and controlled by a sizable number of secondary devices and schemes that make up the cyber layer of a power system. In the cyber layer, auxiliary devices are equipped with communication, data collection, storage, processing, decision-making, control actuation initialization, etc. capabilities. They could be sophisticated electrical gadgets or more potent hardware that can run applications for business at a local market or command center. Cyber-layer elements may be linked over open or confidential networks [4].

II KEY CONSIDERATIONS FOR INTRUSION DETECTION IN SMART POWER GRIDS

Network Traffic Monitoring: Monitoring network traffic within the smart grid system serves as the first step in intrusion detection. To do this, data must be gathered from a variety of networked devices, including sensors, smart meters, and control systems. Techniques like packet capture or network flow analysis can be used to collect the data.

Anomaly Detection: Techniques for anomaly detection are employed to spot departures from typical behavior. Abnormal activity in the context of smart power grids could include strange communication patterns, abnormal network traffic, or strange energy consumption patterns. To find such abnormalities, statistical techniques, machine learning algorithms, or expert systems can be used.

Signature-based Detection: A database of recognized attack signatures or patterns is the foundation of SDS (Signature-Based Detection). Recognize and categorize attacks, it includes comparing the observed network traffic against a database of predetermined signatures. This method works well for identifying known attacks, but it may have trouble identifying brand-new or unidentified attacks.

Intrusion Prevention Systems (IPS): IPS can be used to perform an active response to threats discovered in addition to intrusion detection. IPS can automatically take preventive actions including blocking or isolating suspect network traffic, limiting access, or sending network administrators notifications.

Secure Communication Protocols: Making sure that the various parts of the smart grid infrastructure use secure communication protocols, such as encryption and authentication procedures, helps prevent unauthorized access and data tampering. Systems for detecting intrusions can keep an eye on how these protocols are being used and spot any irregularities or tries to bypass security.

Integration with Security Information and Event Management (SIEM): The entire smart grid infrastructure can be centrally monitored, corroborated, and analyzed for security events thanks to the integration of intrusion detection systems with SIEM platforms. SIEM systems offer a comprehensive view of security occurrences, simplify incident response, and enhance regulatory compliance.

Continuous Monitoring and Updates: To successfully detect and destroy evolving threats, IDS should be regularly updated with the most recent threat intelligence, attack signatures, and vulnerability information. It is essential to continuously monitor the smart grid infrastructure to quickly detect and respond to any potential security events or attacks.

III RELATED WORKS

A smart grid is a cyber-physical structure that uses functional automation in ICT (Information and Communication Technologies) to improve the functionality of conventional electricity networks. These technologies enable energy supply firms to deliver dependable power at a reasonable cost with few losses. Despite the benefits, such cyber-physical systems are vulnerable to diverse attacks that compromise the confidentiality and integrity of data. IDS are recommended as a practical remedy in a substantial portion of the research that tries to address these shortcomings of the smart grids. However, the main issues with such systems are their robustness, precision, and adaptation to new threats. Dinesh Mohanty et al.'s proposal of a DRL(Deep Reinforcement Learning) based intelligent IDS for smart grid networks was made in response. This suggested IDS is reliable, extremely accurate, and has a minimal false alarm rate. It is built on the cutting-edge CVAEDDQN framework, which integrates a generative model and DRL. The authors chose the standard network-based NSL-KDD dataset and the cloud-specific ISOT-CID dataset because there aren't any datasets specifically designed for the smart grid. The research outcomes demonstrate our suggested system's efficacy in terms of accuracy rate, false positive rate, and network attack detection capabilities. They have also assessed this model's adaptability to changes in attack behaviors and major attack kinds[5].

The future generation of power systems, known as "smart grids," would be sophisticated and capable of monitoring both on-site and remote activity. It has to be able to identify cyberattacks in a timely and efficient manner because it is a cyber-embedded infrastructure. This Tong Yuet al., 2022 attempt attempts to offer an advanced and distinctive intrusion detection model capable of categorizing electrical network incidents and CDs for smart grids into binary-class, trinary-class, and multiple-class categories. As an effective ML model for intrusion detection, it uses the grey wolf algorithm (GWA) for adaptive training of ANN (Artificial Neural Network). For to achieve the lowest MSE (Mean Square Error), the weight vectors of the intrusion detection model are initialized and modified using the GWA. The challenges of cyber-attacks, failure forecasting, and failure diagnosing in the smart grid energy industry would be effectively tackled with the recommended growing ML model. The suggested model is demonstrated, and the explanation of the experimental findings is provided, using a real dataset from the Mississippi State Laboratory in the United States. The suggested model is contrasted with a few of the most popular classifiers in the field. According to the findings, the recommended intrusion detection model works better than other popular systems in this area [6].

Modern system privacy and defense mechanisms have been greatly improved with the application of ML-based IDS methods. Security risks have greatly increased in smart grid computing settings as a result of the widespread use of shared networks and the resulting dangers. However, in comparison to other network settings, research on ML-based IDS in a smart grid is comparatively underdeveloped, even though the environment of the smart grid is vulnerable to major security threats because of its particular environmental flaws. The authors of this article, Nitasha Sahani et al., 2023, carried out a thorough analysis of ML-based IDS in smart grids based on several crucial factors: (1) the potential uses of ML-based IDS in transfer and distribution side power elements of a smart power grid by addressing its privacy flaws; (2) the dataset generation procedure and its use for deploying ML-based IDSs in the smart grid; (3) an extensive variety of ML-based IDSs utilized by the investigated articles in the smart grid setup; (4) metrics, additional complexity evaluation, and assessment test beds of the IDSs utilized in the smart grid; and (5) lessons obtained, insights.[7]

Chunhe Song et al., 2021 proposed a novel intrusion detection method combining a deep learning-based method and a feature-based method for smart grids. Specifically, long short-term memory and extreme gradient boosting are adopted for intrusion detection, and the results are fused based on the accuracies of these two models. As the XGBoost method is sensitive to its parameters and unsuitable selections greatly degrade its performance, in this paper, a Bayesian method is proposed to optimize these parameters. Moreover, a crossover scheme in a genetic algorithm is introduced to reduce the impact of falling into a local optimum of Bayesian optimization. Extensive experimental results show the effectiveness of the proposed algorithm [8].

Due to the smart grid's susceptibility to network attacks, IDSs must have a high rate of detection and quick detection times. The ELM (Extreme Learning Machine) completely satisfies the requirements of intrusion detection of the smart grid thanks to its quick training speed and high model generalization ability. Ke Zhang et al., 2020 used ELM in the discipline of smart grid intrusion detection in this work. A GA-ELM approach based on a GA is suggested to address the issue that the randomness of input weights and unseen layer bias in the ELM cannot ensure the best performance of the ELM IDS model. The input weight and unseen layer bias of the ELM are optimized using GA. A GA's chromosomal vector is first mapped to the input weight and unseen layer bias of the ELM, and the test error value of the ELM model is configured as the fitness coefficient of the GA. Then, the input weight value and bias, which correlate to the least test error, are chosen to enhance the functionality of the ELM system. The variables of the ELM IDS model are then optimized by the genetic procedure. The GA-ELM successfully increases the accuracy rate, detection rate, and precision of intrusion detection while lowering the false positive rate and missing report rate when compared to the ELM and online sequential extreme learning machine (OS-ELM)[9].

A smart grid based on a three-layer communication hierarchy structure is described by Slavica Botjani Rakas et al. in 2019. Such a network must contend with several cyber security issues, which could seriously affect the power system. The cyber security of the smart grid has been handled with a summary of its flaws and threats. IDS, with an emphasis on detection methods and characteristics that reflect the efficacy of the IDS, has been viewed as one of the most successful approaches to avoid these types of attacks. The prerequisites for applying IDSs in a smart grid setting have been defined, [10].

The capacity of traditional power system networks is usually enhanced by smart grid systems as they are more susceptible to various types of attacks. These flaws could allow hackers or intrusions to bring down the entire network, security, and confidentiality of smart grid systems. To provide a trustworthy and secure range of services within the smart grid framework, IDS is crucial. There are multiple current methods for detecting assaults in the smart grid system, but they use an outdated dataset to identify anomalies, which reduces their rate of recognition effectiveness in real-time and large data sources.

P. Ganesa et al.'s suggested approach, which uses both real-time raw data from the smart grid infrastructure and KDD99 dataset for identifying abnormalities in the smart grid network, is provided in 2022 as a solution to these shortcomings. By eliminating distribution line distortion, the power sent to the grid is inspected and improved in terms of reliability during the grid-side data-gathering process. In this method, the defect is corrected using a FACT device called the UPQC (Unified Power Quality Controller), which then stores the data in a cloud server, improving the power performance of the smart grid network. Improved Aquila Swarm Optimization (IASO) is used to pre-process and optimize the data from a given dataset to obtain the best characteristics. After that, PRRN (Probabilistic Recurrent Neural Network) classifier is used to predict and categorize incursions. In the context of grid voltage, grid current value, total harmonic distortion (THD) data, voltage sag/swell, accuracy rate, precision, recall, F-score, FAR(false acceptance rate), and the detection efficiency of the classification algorithm, the performance is finally calculated and the results are forecasted. To verify the effectiveness of the suggested model, the analysis is contrasted with currently used methodologies [11].

The AMI (Advanced Metering Infrastructure) and smart meters used in the smart grid enable the communication of real-time information between the utility provider and the user. The smart grid is the next-generation power grid model. Numerous services for both are made possible by these data, including time-of-use (TOU) pricing, demand side administration, and automatic meter readings. However, because smart grid systems are constructed using both cutting-edge and antiquated information and operational technology, there has been an increase in concerns regarding confidentiality and security. For smart grid systems, intrusion detection is a crucial safety feature that warns the system controller of the existence of active attacks. As a result, intrusion detection has been the subject of extensive research, particularly anomaly-based intrusion detection. When standard pattern recognition techniques are applied to data that is unbalanced and contains far more instances of normal behaviors than of attack behaviors, problems arise since these techniques have low detection rates for minority classes. Using the

CIC-IDS2018 dataset, Dipanjan Das Roy et al., 2019 investigate various ML algorithms to address this issue [12].

IV PROPOSED METHODOLOGY

The suggested paradigm for smart grid intrusion detection entails several processes. First, SMOTE, PCA, Min-Max scaling, and Z-score normalization are used to preprocess the dataset. By creating synthetic samples of the minority class, SMOTE is used to address the problem of class imbalance. To reduce the number of features while retaining the most crucial data, dimensionality reduction using PCA is used. The feature values are normalized using Min-Max scaling and Z-score normalization to maintain uniformity across scales.

After preprocessing, the SVM method is used to carry out the classification task. SVM is an effective machine learning technique that excels at solving binary classification issues. By maximizing the margin between the two classes, it looks for an ideal hyperplane to divide them. The proposed model attempts to enhance the accuracy of intrusion detection in smart grids while reducing false positives by combining these preprocessing techniques and SVM classification. The model decreases dimensionality, accounts for the dataset's imbalance, and makes use of SVM's advantages in binary classification. Figure 2 below depicts the overall layout of the suggested system.

Data set Collection

To recognize and prevent unauthorized access or malicious activity, the process of obtaining data from numerous sources within a smart grid is known as intrusion detection. Determine the various smart grid system data sources that produce information useful for intrusion detection. Smart meters, SCADA systems, wireless networks, and other hardware or sensors maybe some of these sources.

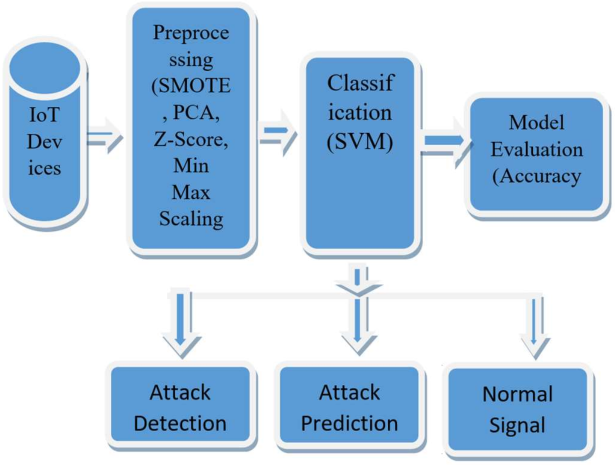
IoT Dev ices
Preproce ssing (SMOTE , PCA, Z-Score, Min Max Scaling
Classif ication (SVM)
Model Evaluation (Accuracy
Attack Detection
Attack Prediction
Normal Signal

Fig 2 Outline of the Proposed Framework

Preprocessing

Z-Score

Z-score normalization, also known as attribute scaling using standardization, is a crucial pre-processing step in many ML techniques. Rescaling parameters that have the characteristics of a standard normal distribution with a mean value of zero and a value of SD (Standard Deviation) as one is a step in the standardization process [13]. When calculated in SD units, a Z-score shows the location of a raw score depending on how much it deviates from the mean value. Positive Z-score values are those that are above the mean value, while negative Z-score values are those that are below the mean value. Because it standardizes the distribution, this technique, also known as normal score, enables the evaluation of scores on multiple types of identifiers. The simple Z-score is calculated using the formula (1). It is just the raw scoreless population mean divided by the population SD [14].

$$Z = \frac{x - \mu}{\sigma} - - - (1)$$

Where Zrepresents the standard score value,xis the observed value, μis the mean value of the sample and σis the SD of the sample.

Z-score normalization is used to standardize the feature values of the dataset before executing the intrusion detection task in smart grids with Z-score preprocessing. It is advantageous to use Z-score preprocessing for intrusion detection in smart grids because it improves feature interpretation, outlier detection, convergence, and robustness to skewed distributions. It helps to create an intrusion detection system that is more accurate and understandable.

SMOTE

SMOTE [15] is a crucial method that creates balanced datasets by oversampling the minority class. By practicing each minority class sample and incorporating synthetic samples along the line segments joining any/all of the k minority class nearest neighbours, it oversamples the minority class. The k-nearest neighbours are selected at random, according to the quantity of oversampling required [16].

Below is a detailed description of the SMOTE algorithm:

For each sample, determine the k-nearest neighbours.

Choose samples at random from the k-nearest neighbour

Calculate the new samples using the formula: original samples + difference * gap (0,1)

Expand the minority with new samples. A fresh dataset is subsequently produced.

To perform intrusion detection in smart grids with SMOTE pre-processing, SMOTE is used to address the problem of class imbalance in the dataset. By addressing the issue of class imbalance by using SMOTE as a pre-processing strategy for intrusion detection in smart grids, model performance, generalization, and intrusion detection accuracy are all increased.

Min Max Scaling

The Min-Max scalar is an additional method for normalizing the input features and parameters. As a result, all features will be converted into a range [0,1], with 0 and 1 serving as the minimum and maximum values of each feature/ variable, respectively[17].Before conducting the classification assignment, the Min-Max scaling technique is used to normalize the feature values of the dataset for intrusion detection in smart grids. The pre-processing method known as normalization, often referred to as min-max scaling, is frequently used to scale numerical features within a given range, usually between 0 and 1.

$$x_{scaled} = \frac{x - \min(x)}{\max(x) - \min(x)} - - - - - - -(2)$$

In smart grid intrusion detection, using Min-Max scaling as a preprocessing strategy has benefits like better feature scaling, quicker convergence, robustness to outliers, and increased model interpretability. It supports a just and efficient classification process, enhancing the security and dependability of smart grid systems.

PCA (Principal Component Analysis)

A well-liked unsupervised learning method for lowering the dimensionality of data is PCA. While minimizing information loss, it simultaneously improves interpretability. It makes data easier to plot in 2D and 3D and aids in identifying the dataset's most important properties. The PCs(Principal Components) are a line that captures the majority of the data variance. They have a magnitude value and a direction. The orthogonal (perpendicular) projections of data onto lower-dimensional space are the PCs[18].

Steps

Dataset Standardization

It is necessary to compute the mean and SD for each attribute to standardize the dataset. The formula for standardization [19] is:

$$x_{new} = \frac{x - \mu}{\sigma} - - - - - (3)$$

Make the covariance matrix calculations for the entire dataset.

The covariance matrix is computed using the following formula:

For population

$$Cov(x, y)\frac{\sum(x_i - \bar{\bar{x}}) * (y_i - \bar{y})}{N} - - - - - - -(4)$$

For Sample

$$Cov(x, y)\frac{\sum(x_i - \bar{\bar{x}}) * (y_i - \bar{y})}{(N - 1)} - - - - - - -(5)$$

Do the eigenvalue and eigenvector calculations.

Once the linear transformation is utilized to a nonzero vector, an eigenvector is a vector that changes by a scalar amount at most. The eigenvector's scaling factor is determined by the matching eigenvalue.

Order the eigenvalues and eigenvectors that go with them.

Create an eigenvector matrix using k eigenvalues.

The original matrix be transformed

Before executing the intrusion detection task, the dataset's dimensionality is reduced using PCA in smart grid intrusion detection. Smart grid intrusion detection using PCA as a preprocessing method has advantages such as dimensionality reduction, improved computational efficiency, noise reduction, feature selection, and an understandable representation of the data.

Classification using SVM

A classification technique for both linear and nonlinear data is the SVM. The original training data is conducted to a higher dimension using nonlinear mapping. In terms of widely used algorithms, it is a pretty accurate technique. It develops quickly in a two-class learning assignment.SVM seeks to identify the best classification function to distinguish between individuals belonging to the two classes in the training set.

The linear SVM strategy can be expanded to create a nonlinear SVM for the classification of linearly indivisible data if the data are not linearly divided. The original data input is transformed into a higher dimensional space using a nonlinear mapping in the nonlinear SVM strategy, and then a linear hyperplane is searched for in the new space[21].

A hyperplane equation is the name given to the equation for the major separator line. The equations are:

$$mx + c = 0 - - - - - - - - (6)$$

Here m denotes slope and c indicates intercept value.

Now it is simple to write the hyperplane equation separating the points (for classification) as:

$$H : W^T(x) + b = 0 - - - - - - (7)$$

Here, b is the hyperplane equation's interception and bias component.

A common method for identifying and separating typical from abnormal network behaviors is intrusion detection classification using SVM. To clearly define the boundary between the two classes, it seeks to maximize the margin between them. SVM's capacity to handle high-dimensional feature spaces, handle both linear and non-linear separations through kernel functions, and be effective when dealing with imbalanced datasets are just a few benefits of utilizing SVM for intrusion detection classifying.

V RESULTS AND DISCUSSION

Significant results were obtained using the intrusion detection smart grid preparation technique, which handled imbalanced datasets using SMOTE, reduced dimensions using PCA, scaled features using Min-Max with Z-score normalization, and then classified data using SVM. The strategy aims to improve intrusion detection systems' detection precision and reduce false positives. The trial outcomes revealed appreciable advancements in both areas.

By creating synthetic samples of the minority class, SMOTE's application successfully balanced the dataset, boosting the representation of incursion instances. PCA improved classification accuracy by reducing the dimensionality of the feature space while keeping the most crucial data. Furthermore, the features were standardized and consistent across various scales and distributions because of the combined use of Min-Max scaling and Z-score normalization, which facilitated correct categorization. The SVM classifier showed that it was adept at handling binary classification problems, improving detection precision, and lowering false-positive rates.

Model Evaluation:

Accuracy Analysis: Accuracy measures the general accuracy of the model's predictions by comparing the percentage of correctly classified f samples to all samples. It provides a thorough assessment of the model's performance.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} - - - - - - - - (8)$$

Table 1: Accuracy Analysis of SMOTE-SVM with other Existing Algorithms

No of Iterations	PCA-SVM Accuracy (%)	Min-Max-SVM Accuracy (%)	Z Score-SVM Accuracy (%)	SMOTE-SVM Accuracy (%)
10	85.26	86.76	88.99	89.79
20	85.86	87.21	89.3	90.16
30	86.21	87.5	89.71	90.56
40	86.82	87.98	89.90	90.81
50	86.98	88.95	89.96	90.90

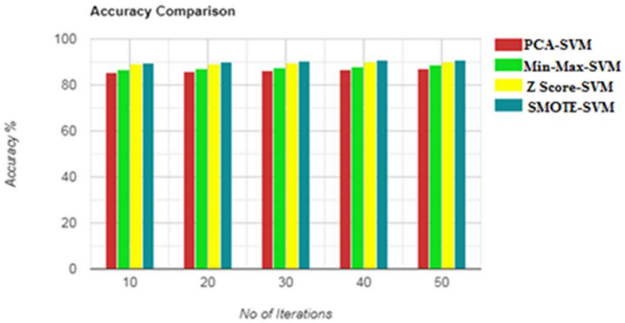

Fig 3 Accuracy Analysis of SMOTE-SVM with other Existing Algorithms Graph

Precision Analysis: When compared to all samples that were predicted to be positive (including true and false positives), precision is the percentage of positively recognized positive samples (also known as true positives). When classifying intrusion datasets, precision relates to how well the model can recognize certain anomalies. Precision is defined as the ratio of genuine positives to all predicted positives.

$$Precision = \frac{TP}{TP + FP} - - - - - - - - (9)$$

Table 2: Precision Analysis of SMOTE-SVM with other Existing Algorithms

No of Iterations	PCA-SVM Precision	Min-Max-SVM Precision	Z Score-SVM Precision	SMOTE-SVM Precision
10	0.82	0.84	0.85	0.86

20	0.84	0.85	0.85	0.87
30	0.84	0.85	0.85	0.89
40	0.84	0.85	0.86	0.90
50	0.84	0.85	0.86	0.91

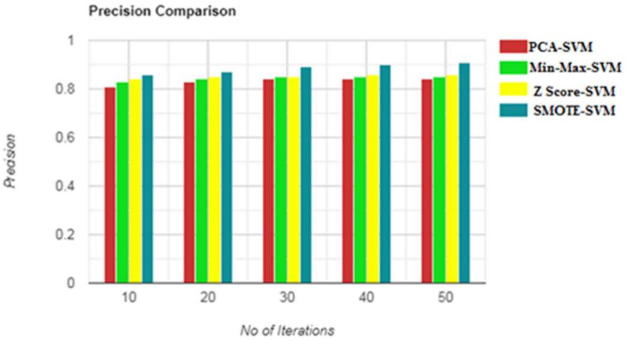

Fig 4 Precision Analysis of SMOTE-SVM with other Existing Algorithms Graph

Recall Analysis: The percentage of positive samples that are correctly identified as such (true positives) from the overall number of positive samples (true positives plus false negatives) is known as recall, also known as sensitivity or true positive rate. It illustrates the model's ability to recognize each instance of a certain threat.

A recall is exactly the ratio of true positives to all of the positives in the ground truth.

$$Recall = \frac{TP}{TP + FN} - - - - - - - - (10)$$

Table 3: Recall Analysis of SMOTE-SVM with other Existing Algorithms

No of Iterations	PCA-SVM Recall	Min-Max-SVM Recall	Z Score-SVM Recall	SMOTE-SVM Recall
10	0.77	0.80	0.82	0.84
20	0.77	0.82	0.83	0.85
30	0.77	0.82	0.83	0.85
40	0.77	0.83	0.84	0.86
50	0.79	0.83	0.84	0.86

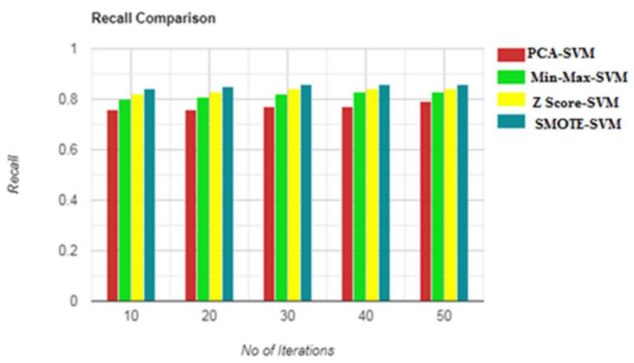

Fig 5 Recall Analysis of SMOTE-SVM with other Existing Algorithms Graph

The proposed model, which addresses major issues and makes use of cutting-edge approaches to improve the precision and efficacy of the detection system offers a comprehensive approach to intrusion detection in smart grids.

The suggested preprocessing pipeline and classification method have shown their promise for efficient intrusion detection in smart grids, enhancing the infrastructure's security and dependability. The significance of thorough preprocessing methods and the applicability of SVM for intrusion detection in smart grid scenarios are highlighted by these results.

VI CONCLUSION

To guarantee the security and dependability of the power grid infrastructure, intrusion detection in smart grids is a crucial task. To address the imbalanced nature of the dataset and reduce dimensionality while preserving important information, a preprocessing pipeline consisting of SMOTE, PCA, and Min-Max scaling with Z-score normalization was applied in this study. The SVM approach, which has shown to be successful in tackling binary classification issues, was used to solve the classification challenge. The experimental outcomes showed that the suggested method improved detection precision and decreased false positives, making it a promising intrusion detection method for smart grids. The performance of the suggested approach can be assessed on larger and more varied datasets in future studies, and other cutting-edge machine-learning techniques can be investigated for comparison.

REFERENCES

[1] Chongrui Tian, Fengbin Zhang, Zhaoxiang Li, Ruidong Wang, Xunhua Huang, Liang Xi& Yi Zhang(2022), “Intrusion Detection Method Based on Deep Learning“, Wireless Communications and Mobile Computing, Vol. 2022, | Article ID 1338392, https://doi.org/10.1155/2022/1338392.

[2] Bojja Pranitha, KesapragadaVenkata Rama AnirudhVikram, Balabhadruni Anil, KaranamKiranSai& P. Anuradha(2022), “Detection of Smart Grid Attacks Using Machine Learning Techniques”, Journal of Engineering Sciences, Vol 13, No. 04, pp. 444-454.

[3] Arun Sekar Rajasekaran, P. Kalyanchakravarthi & Partha Sarathi Subudhi(2022), “Anomaly Detection of Smart Grid Equipment Using Machine Learning Applications“, Distributed Generation & Alternative Energy Journal, Vol.37, No. 5. https://doi.org/10.13052/dgaej2156-3306.37518

[4] Pengyuan Wang & Manimaran Govindarasu(2019), “Cyber-Physical Anomaly Detection for Power Grid with Machine Learning”, Springer Industrial Control Systems Security and Resiliency, pp 31–49

[5] Dinesh Mohanty, KamalakantaSethi, SaiPrasath, RashmiRanjan Rout&PadmalochanBera(2021), “Intelligent Intrusion Detection System for Smart Grid Applications“,2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2021, pp. 1-8, doi: 10.1109/CyberSA52016.2021.9478200.

[6] Tong Yu, Kai Da, Zhiwen Wang, Ying Ling, Xin Li, Dongmei Bin1 &ChunyanYang(2022), “An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning“, Front. Energy Res., 30 May 2022 Sec. Smart Grids,Vol. 10 – 2022, https://doi.org/10.3389/fenrg.2022.903370

[7] NitashaSahani, Ruoxi Zhu Jin-HeeCho, Chen-Ching Liu(2023), “Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey“, ACM Transactions on Cyber-Physical Systems, Vol. 7, No. 2 Article No.: 11, pp 1–31, https://doi.org/10.1145/3578366

[8] Chunhe Song a, Yingying Sun a d, Guangjie Han b c, Joel J.P.C. Rodrigues (2021), Intrusion detection based on hybrid classifiers for smart grid “, Science Direct “Computers & Electrical Engineering, Vol. 93, July 2021, 107212

[9] Ke Zhang, Zhi Hu, YufeiZhan&Xiaofen Wang (2020), “A Smart Grid AMI Intrusion Detection Strategy Based on Extreme Learning Machine“, Energies, Vol.13, No, 18. 10.3390/en13184907

[10] SlavicaBoštjančičRakas, Valentina Timčenko, MilenkoKabović& AnkaKabović(2022),“Intrusion Detection Systems in Smart Grid“, Infoteh-Jahorina (Infoteh), East Sarajevo, Bosnia and Herzegovina, 2022, pp. 1-6, doi: 10.1109/INFOTEH53737.2022.9751302.

[11] P. Ganesan & S. Arockia Edwin Xavier(2023), “An Intelligent Intrusion Detection System in Smart Grid Using PRNN Classifier“, IASC/ Vol.35, No.3, 2023/ 10.32604/iasc.2023.029264

[12] Dipanjan Das Roy &Dongwan Shin(2019), “Network Intrusion Detection in Smart Grids for Imbalanced Attack Types Using Machine Learning Models”, IEEE ICTC 2019, pp. 576-581.

[13]https://scikit-learn.org/stable/auto_examples/preprocessing/ plot_scaling _importance. HTML #:~: text= Feature%20scaling%2 0 through%20 standardization%20(or,a%20standard%20deviation%20of%20one.

[14] Dr. Saul McLeod(2019), “Z-Score: Definition, Calculation and Interpretation “, https://www.simplypsychology.org/ z-score.html

[15] N.V. Chawla, K.W. Bowyer, L.O. Hall &W.P. Kegelmeyer, “Smote: Synthetic Minority Over-Sampling Technique”, J. Artif. Intell. Res., Vol. 16, 2002, pp. 321-357.

[16] Ahmed Saad Hussein, Tianrui Li, Chubato Wondaferaw Yohannese & Kamal Bashir(2019), “A-SMOTE: A New Preprocessing Approach for Highly Imbalanced Datasets by Improving SMOTE“, International Journal of Computational Intelligence Systems, Volume 12, Issue 2, 2019, Pages 1412 – 1422

[17] Serafeim Loukas(2020), “Everything you need to know about Min-Max normalization: A Python tutorial“, Towards Data Science.

[18]https://www.simplilearn.com/tutorials/machine-learning-tutorial/principal-component-analysis

[19]https://medium.com/analytics-vidhya/understanding-principle-component-analysis-pca-step-by-step-e7a4bb4031d9

[20]https://www.analyticsvidhya.com/blog/2019/08/11-important-model-evaluation-error-metrics/

[21] Abdulhamit Subasi,Khloud Al-Marwani, Reem Alghamdi, Aisha Kwairanga& Saeed M. Qais(2018), "Intrusion Detection in Smart Grid Using Data Mining Techniques ",Intrusion Detection in Smart Grid Using Data Mining Techniques," 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 2018, pp. 1-6, doi: 10.1109/NCG.2018.8593124.

[22] Ruobin Qi, Craig Rasband, Jun Zheng&Raul Longoria(2021), "Detecting Cyber Attacks in Smart Grids Using Semi-Supervised Anomaly Detection and Deep Representation Learning", MDPI Information, Volume 12 Issue 8 10.3390/info12080328

2