Protection of a smart grid with the detection of cyber- malware attacks using efficient and novel machine learning models

frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 05 August 2022
DOI 10.3389/fenrg.2022.964305

OPEN ACCESS

EDITED BY
Xueqian Fu,
China Agricultural University, China

REVIEWED BY
Muhammad Aamir,
Huanggang Normal University, China
Muhammad Mateen Afzal Awan,
University of Management and Technology, Pakistan
Muhammad Jehanzeb Irshad,
University of Gujrat, Pakistan

*CORRESPONDENCE
Jianbin Wu,
wjb@zjnu.cn

SPECIALTY SECTION
This article was submitted to Smart Grids,
a section of the journal
Frontiers in Energy Research

RECEIVED 08 June 2022
ACCEPTED 27 June 2022
PUBLISHED 05 August 2022

CITATION
Aziz S, Irshad M, Haider SA, Wu J, Deng DN and Ahmad S (2022), Protection of a smart grid with the detection of cyber- malware attacks using efficient and novel machine learning models.
Front. Energy Res. 10:964305.
doi: 10.3389/fenrg.2022.964305

Protection of a smart grid with the detection of cyber- malware attacks using efficient and novel machine learning models

Saddam Aziz[1], Muhammad Irshad[2], Sami Ahmed Haider[3], Jianbin Wu[4]*, Ding Nan Deng[5] and Sadiq Ahmad[6]

[1]Centre for Advances in Reliability and Safety, New Territories, Hong Kong, China, [2]Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China, [3]Department of Computing, University of Worcester, Henwick Grove, United Kingdom, [4]Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua, China, [5]School of Physics and Electronic Engineering, Jiaying University, Meizhou, China, [6]ECE Department COMSATS University Islamabad, Wah Cantt, Pakistan

False data injection (FDI) attacks commonly target smart grids. Using the tools that are now available for detecting incorrect data, it is not possible to identify FDI attacks. One way that can be used to identify FDI attacks is machine learning. The purpose of this study is to analyse each of the six supervised learning (SVM-FS) hybrid techniques using the six different boosting and feature selection (FS) methodologies. A dataset from the smart grid is utilised in the process of determining the applicability of various technologies. Comparisons of detection strategies are made based on how accurately each one can identify different kinds of threats. The performance of classification algorithms that are used to detect FDI assaults is improved by the application of supervised learning and hybrid methods in a simulated exercise.

KEYWORDS

smart grid, cyber-attack, false data injection, feature selection, classification algorithms

1 Introduction

Powerful Smart Grid solutions are on the verge of disrupting the current industries with their ability to improve the efficiency of traditional electric networks. A digital communications-based energy supply grid is known as the "Smart Grid" (Mollah et al., 2021), (Aziz et al., 2017). Increased demand has led to problems such as blackouts, overheating, and voltage drops. Additionally, the existing electrical network has seen an increase in carbon emissions that is critical to mitigating the cyber-attack (Sakhnini et al., 2019). Up to 40% of the country's CO2 emissions are absorbed by the United States, which is bad for the environment (Case et al., 2021). The Smart Grid will incorporate cutting-edge communication and calculation capabilities, all of which are projected to enhance the system's efficiency, reliability, and availability (Ruan et al., 2017).

A second advantage of a Smart Grid is its capacity to converse with itself (Majeed Butt et al., 2021), (Sami et al., 2022). The Smart Grid's history includes natural gas, coal, fossil fuels and renewable energy sources including wind turbines and solar panels (Wang et al., 2020). The Smart Grid's efficient power distribution and use can benefit a wide range of smart devices, transformers, and machinery. It accomplishes these goals by using two-way communication instead of the typical grid system's one-way communication. Faster and better services for customers can be achieved through the Smart Grid, allowing for a quick implementation of the energy problem (Wu et al., 2021).

However, Smart Grid technology has weaknesses and obstacles, the most notable of which is the inability to preserve the most vital asset, data. The Smart Grid will need to share data on a regular basis since sensitive information may be stored there (Moghadam et al., 2020). The Smart Grid Many gadgets, both commercial and domestic, will be linked via a variety of networks in order to communicate and provide security to the networks utilising various techniques to cyber security. Smart Grid cyber security is critical. An evaluation and analysis of various security measures will be done in order to find a solution to these complex concerns (Aziz et al., 2022), (Chehri et al., 2021). A "smart grid" is a system that employs communication and information technologies to generate, distribute, and consume electric power. New functionalities such as real-time control and operational efficiency as well as increased grid resilience as well as the integration of renewable technologies to reduce carbon footprint (Ma et al., 2020) are achieved through the use of two-way information flow. There are, however, some drawbacks to using a smart grid.

If a power loss happens, the stability of the smart grid could be compromised, and the socioeconomic consequences could be considerable (Murthy et al., 2022). As a result of theft or manipulation of important data exchanged across smart grid systems, users' privacy may potentially be violated. Since these problems have been discovered, the smart grid has gained the interest of both government agencies and private sector companies. An increasing number of attacks against smart grids are being carried out using a technique known as False Data Injection (FDI) (Hu et al., 2021).

It's impossible to catch sly FDI attacks using today's poor data detection methods (Akram et al., 2021). Machine learning has been proposed as an alternative to FDI detection. The first time the term "false data injection attack" (FDIA) surfaced was in relation to the smart grid (Tan et al., 2017). There are several ways an attacker can tamper with sensor readings to introduce unnoticed errors into state variables and values despite the term's resemblance to "tampering." Using an injection attack, malicious input can be injected into a web application and compelled to do specific commands. An injection attack has the potential to compromise a web server as a whole and cause a denial of service attack (Ye and Lin, 2010; Abu Hussein et al., 2014; Tarafdar Hagh et al., 2015; Li et al., 2021).

A machine learning approach is being developed to detect and safeguard the smart grid from fraudulent data injection in this study. A combined machine learning and feature selection strategy is being proposed. The primary goals of this investigation are:

1) To propose hybrid models for the protection and detection of cyber-attacks in smart grid stations.
2) To implement hybrid techniques using generic supervised machine learning models.
3) To evaluate and compare the proposed model on the basis of accuracy precision, recall and F1 score.

Sections have been numbered from one to five in this work. The study's introductory section can be found in Section 1. The related work is shown in Section 2, and the methodology and data collection are shown in Section 3. Section 4 details the current study's implementation and results, while Section 5 concludes the investigation.

2 Related work

False Data Injection (FDI) attacks are a common sort of cyber-attack on smart grids (Sargolzaei et al., 2020). It's impossible to catch FDI attacks that use shoddy data detection technologies nowadays. In the past, it has been argued that machine learning may be used to detect attacks on foreign investment (FDI). This study (Sakhnini et al., 2019), which focuses on three different supervised learning techniques, examines each of the three different feature selection (FS) methodologies. IEEE 14-, 57-, and 118-bus systems are used to test the applicability of these techniques. Detection methods are compared based on how accurate they are in detecting specific threats. When supervised learning and heuristic FS techniques (Al-Sahaf et al., 2019) are combined in a simulation, FDI attack detection systems perform better.

Stacked Auto Encoders (SAEs) can be used to construct machine-learned characteristics against transmission SCADA attacks as a supplement to more high-quality features, according to Wilson et al. (2018). Compared to current ML detection systems, this framework exploits the automaticity of unsupervised feature learning to reduce the dependency on system models and human knowledge in complex security scenarios. SCADA intrusions in power transmission systems can be detected using machine-learned characteristics, as demonstrated by simulations from a high-fidelity smart grid test bed. A typical SCADA-based theoretical and applied research on false data injection assaults protection system is shown in the figure below.

As ICT is integrated into the old grid, electric grids are getting smarter. In addition, cyber-attacks on the electrical system may result (Yang et al., 2020). The False Data Injection Attack is one of the most common and damaging threats to the smart grid (FDIA). FDIAs in the grid can be detected using machine learning methods, according to a recent study (Majeed Butt et al., 2021). Several feature selection strategies are put to the test in search of the most accurate features. A variety of machine learning methods are being tested to find the best way to identify such assaults (Irshad et al., 2021). Class distribution in the dataset is skewed, and experiments address this issue. All experiments must be evaluated on their ability to respond quickly in a smart grid.

Attempts to tamper with smart grid power transmission systems by introducing false data are called "false data injection attacks" (Qu et al., 2021). Data-driven machine learning is used in this work (Ashrafuzzaman et al., 2020) to combat state estimation assaults. An ensemble of classifiers is used, and the results are further categorized (Ge et al., 2020). In this strategy, both unsupervised and supervised classifiers are used (Lee et al., 2018). IEEE 14-bus data simulation is utilized to evaluate the algorithm (Boudreaux and Boudreaux, 2018). The outcomes of supervised individual models can be compared to the results of ensemble models. Unsupervised models showed that ensembles outperformed individual classifiers.

Through the use of supervised learning, it is possible to detect malicious communications and estimate their security risks. The term "Internet of Things" refers to the concept of linking billions of physical and technical objects over the internet (Triantafyllou et al., 2018; Long et al., 2022). It is becoming increasingly usual for DoS and spoofing attacks to occur as IoT systems become more popular. This study by Khrishnan et al. (Fu et al., 2020; Sundar et al., 2021) employs three classification algorithms and many supervised feature selection techniques to analyze IoT network data. They are able to accurately predict whether or not IoT devices would be affected by network traffic that is not necessary. It was determined which feature selection algorithms were most effective at predicting network intrusions.

Because of the deterioration of the electrical system, the concept of "smart grids" has become more outmoded. The present smart grid security solutions can detect and stopping known assaults. Their failure to fulfil the most advanced cyber-security standards is disappointing. To combat cyber dangers, you'll need a wide range of tools and strategies. When it comes to spotting unknown risks, a more versatile strategy is needed. With the help of big data analytics, techniques like deep learning, machine learning, and artificial intelligence (AI) may accomplish this. Unknown assaults can be detected by machine learning algorithms that adapt to the baseline behavior of a subject. Machine intelligence and predictive analytics will revolutionize the security business in the future. This study attempts to shed light on some of the issues surrounding the protection of big data and artificial intelligence-based infrastructures. They describe in detail how the modern electrical grid was shaped by technological advances in Chehri and colleagues (Chehri et al., 2021). Qualitative risk evaluation there is a lot of discussion over the dependability, safety, and effectiveness of the network. The author reveals levels when recommending security measures.—e.g. There is also discussion of ways to monitor and collect data.

The traditional electrical grid was transformed into the "smart grid" after a period of transition. Improved reliability, visibility, efficiency, and control can be achieved using the smart grid. It can exchange both energy and information. Communications inside the smart grid are crucial. Smart devices and networks comprise the smart grid. On these networks, DDoS, MITM, and replay attacks are all conceivable. Smart grid fraud has been a growing target for hackers. There are security and vulnerability concerns with the smart grid, according to this study (Rajendran et al., 2019; Fu, 2022). In the closing paragraphs, the attacks are addressed, and answers are offered. The security of the smart grid communication system is discussed in detail in this research. This study help readers comprehend the security challenges connected with smart grid communication systems, networks, and devices.

These attacks, which can cause both bodily and economic devastation, are on the rise. FDIAs on power grid monitoring systems are among them. To influence the estimated condition of the power system, adversaries can carry out FDIAs or modify the system data via compromising sensors. The ability of the energy management system to estimate unknown status factors is critical to its success. Sensor failure detection methods are incorporated into the SE algorithms in order to remove inaccurate data from the gathered measurements. Because BDD modules can not recognize hazardous data vectors introduced by FDIAs in some measures, the SE process's outputs can be affected. Machine learning techniques have increasingly replaced residual based BDD in the detection of unlawful sensor data modification. Comparisons of FDIA detection methods using machine learning and power system SE are made in this article (Sayghe et al., 2020).

Although smart grids use cutting-edge ICT technologies to improve efficiency and resilience, adversaries may exploit new security holes to conduct cyber assaults, resulting in widespread blackouts and infrastructure damage. To better detect attacks on smart grids, supervised learning is widely used, which incorporates training on both regular and malicious events. There must be instances of a variety of attack types in the training dataset for supervised learning to be successful. In order to detect cyber threats in smart grids, this study (Qi et al., 2021) makes use of PMU data. Detection algorithms that can identify previously unknown assaults are trained using just normal events. The author investigated several semi-supervised anomaly detection systems using publically available datasets on power system cyber-attacks. According to

TABLE 1 Comparative of analysis of previous studies.

References	Technique	Dataset	Accuracy (%)	Outcome
Sakhnini et al. (Sakhnini et al., 2019)	Supervised machine learning model and Heuristic feature selection	Smart grid cyber-attack dataset	89.5	Detection of cyber attacks
Wilson et al. (Wilson et al., 2018)	Deep learning models	Power Transmission Systems	91.8	Detection of cyber attacks
L et al. (Mohammadi Rouzbahani et al., 2022)	Multi-Layer Defense Algorithm	Intrusion detection dataset	85.6	Detection of cyber attacks
Sengan et al. (Sengan et al., 2021)	Deep learning	Smart grid cyber-attack dataset	87.01	Detection of cyber attacks

a performance comparison, semi-supervised algorithms outperformed supervised algorithms in recognizing attack events. Semi-supervised anomaly detection systems may benefit from deeper representation learning as well. The authors in (Ruan et al., 2022) propose a data recovery scheme to recover measurements and states contaminated by FDIAs.

Table 1 shows the comparative analysis of previous state of the art research in tabular form:

3 Methodology

Machine learning based Smart Grid Cyber Attack research is still in its infancy due to communication protocols. It's clear that further research is needed in this area. We proposed a Smart Grid cyber-attack security system and solution based on hybrid algorithms. The Logitboosted method's performance features are highlighted for a smart grid system.

The study's major contributions can be broken down into four groups:

1) The present state-of-the-art novel hybrid algorithms for cyber-attack protection and detection system for smart grid on smart grid datasets is to be investigated in this study
2) It's possible to detect attacks in smart grid communication with the use of Hybrid Models.
3) Hybrid models based on cyber-attack detection system models were tested to evaluate how numerical and categorical factors affected their performance.

The current study's planned flow is shown in the diagram below:

3.1 Dataset

False Data Injection (FDI) assaults on the smart grid communication system are all too common. Open source data has been used in this research. Independent and dependent variables can be found in this equation. The features are listed in the following table:

As a user-server approach, the smart grid data interface was developed to make it easier to communicate amongst the various smart grids. The interface accepts crucial data in XML format. On the provider side, this file will also be used as a Hybrid Model parameter.

3.1.1 Data collection and pre-processing

Smart Grid Dataset was used to obtain the raw data. As a result, numerous ways have been used to clean up the data, including deleting duplicates and null entries and so on.

3.1.2 Feature engineering

Data from one domain is utilized to develop functions for learning machines using Feature Engineering. Extracting the most significant properties from raw data, it turns it into machine-learning formats. This study makes use of a correlation matrix to figure out how different variables are related to one another. Based on the MAC address of the mobile device, the model for categorizing mobile devices was established. DHCP servers (Dynamic Host Configuration Protocol) might alter their IP addresses over time, making it difficult to effectively filter traffic to a particular device. A total of 41 mobile devices are monitored for each of their traffic characteristics at the flow level. Packets with comparable source and destination addresses, communication ports and protocols (such as TCP or UDP) are grouped together when it comes to classifying data traffic... Since the packet header provides an aggregated (statistical) view of traffic flow, the source and destination are depicted best. Packet-level traffic analysis necessitates more processing power and storage space. Data packets sent by Google Chrome cast (the device under study) throughout the course of a 24-h period are tied to traffic flow patterns.

3.1.3 Calculation of index feature

As a result of investigations into smart grid communication activities, a phenomenon of predictability in behavior has emerged. The index (C_u) approaches zero, the more predictable it becomes and the less it deviates from the

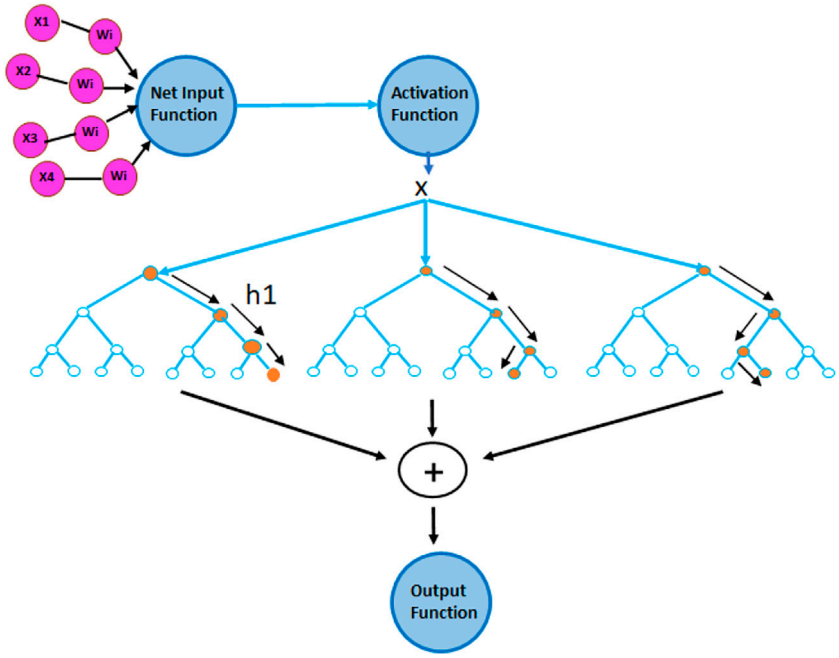

FIGURE 1
Hybrid classifier (SVM-GBC classification) model.

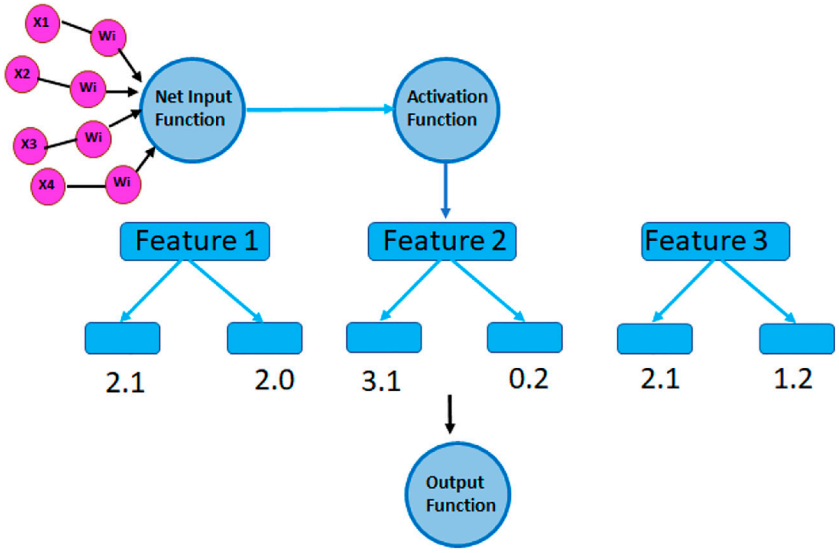

FIGURE 2
Hybrid classifier (SVM-ABC classification) model.

amount of data delivered and received. An index feature can be calculated:

$$C_u = Cvar_u \frac{\sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - x_{i*})^2}}{\frac{1}{N}\sum_{i=1}^{N} x_i} \quad (1)$$

3.1.4 Data pre-processing

The process of translating raw data into usable information is a crucial part of data mining. In many cases, the information we have is inaccurate, inadequate, or just missing. We must fill this void. Based on the C_u index value, the coefficients of variation

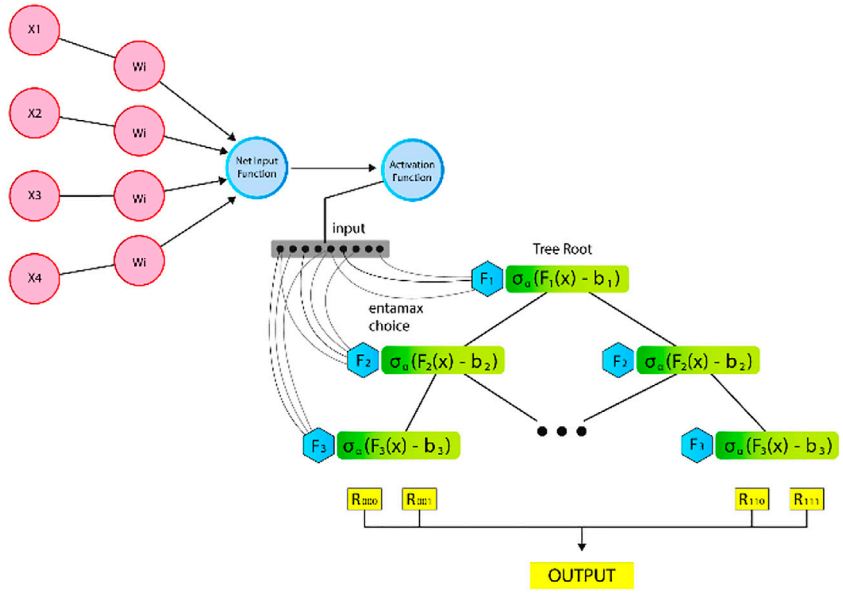

FIGURE 3
Classification Model.Hybrid classifier (SVM-CBC classification) model.

classification method categorized the device types. The data is assumed to have a normal distribution. To make it easier to compare data, the distribution of the obtained values (C_u index) was changed. It was possible to discover the best data transformation function for this study by using the Ladder of Powers approach.

3.1.5 Data normalization

For machine learning, normalization is a standard practice. First, normalize your data to a standard scale without distorting the range of values or sacrificing any data in the process.

3.1.6 Data balancing

Imbalanced classifications stand in the way of precise predictive modelling. The same number of examples are used for each class in machine learning algorithms. The models are inaccurate when it comes to the experiences of people of color. Because the minority group has more influence and is more susceptible to classification errors than the majority, this situation is problematic. As a result, we were able to eliminate the sample's outliers and recalculate the data. New resampling methods have emerged because of this investigation. To save information, we can, for example, sample most class data using sampling and extract records from each cluster. There is no need to replicate minority class data perfectly while sampling synthetic samples; we can make tiny adjustments during the sampling procedure to get more diverse samples. A well-balanced and homogeneous dataset is necessary for data mining research. A dataset may contain "outliers," or data that deviates from the norm. Among a dataset, outliers are those values that deviate significantly from the rest. To deal with an unbalanced dataset, SMOTE was used to normalize the method.

Human mistake, malfunctioning technology, or incorrect data interpretation can all produce outliers. The relevant data must be excluded before any analysis or statistical testing may be performed. Inaccurate or partial results can skew the results of any outliner's analysis and subsequent processing. By using the IQR approach, outliers are removed from data boxplots that fall beyond the method's predefined range. The gap is caused by the difference in IQRs between the upper and lower quartiles. IQR, Z-Scores, and Data Smoothing are some of the statistical approaches used to identify outliers in the data collection. The IQR is calculated by taking the 25th and 75th percentiles from a data set and summing them together.

$$IQR = Q3 - Q1 \tag{2}$$

3.1.7 Hybrid classification algorithms

Limited in the number of ways it can be used to categories things. Using a single procedure, the categorization result is based on solving a variety of problems. Data Injection can be categorized based on how much data is sent between the sender and receiver. The explanations for each model are listed below.

3.1.7.1 SVM-XGB

Both the XGBoost Classifier model and the Support Vector Classifier model were improved by combining them. The

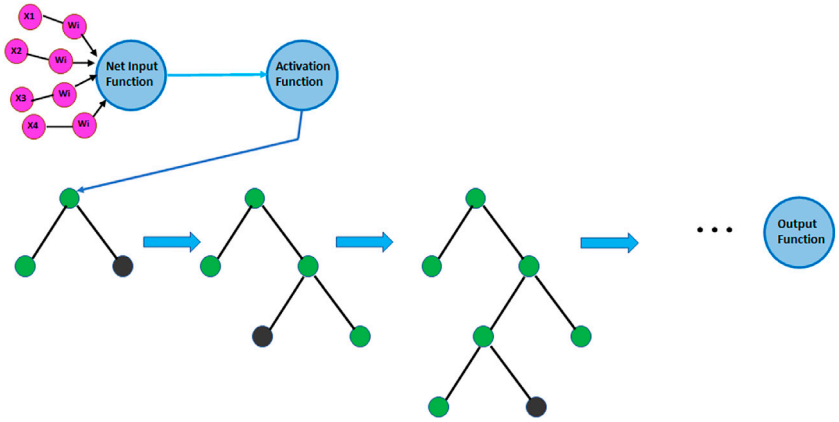

FIGURE 4
Hybrid classifier (SVM-LGBM classification) model.

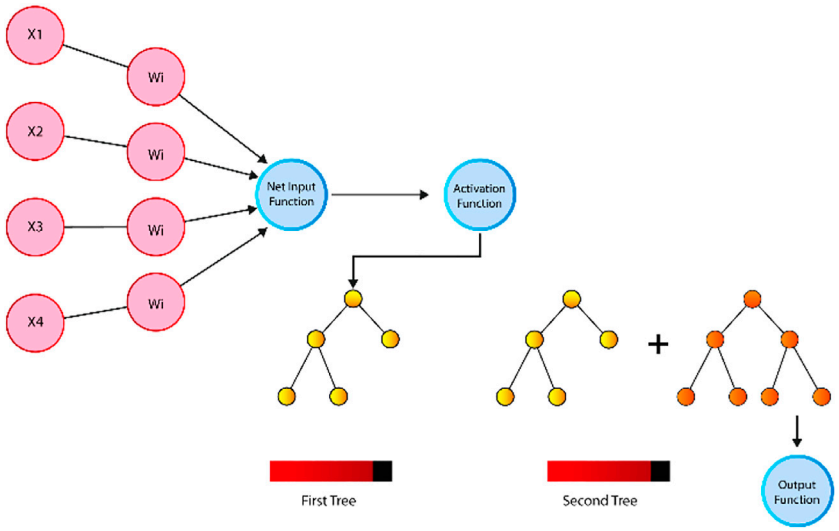

FIGURE 5
Hybrid classifier (SVM-HGBC classification) model.

mathematical model of the SVM-XGB Classification model is as follows:

$$y = \sum_{k=1}^{n} f(x) \tag{3}$$

The support vectors will then be calculated to characterize FDI assaults as follows in the dataset:

$$w.y + b = 1 \ldots (vector\ 1) \tag{4}$$

$$w.y + b = -1 \ldots (vector\ 2) \tag{5}$$

Here w is the hyper plane, y is the output of XGB, and b is the marginal distance. $\sum_{k=1}^{n} f(x)$ XGB Classifier's boosting function is demonstrated here. When XGB receives y's output, it passes it on to the support vector classifier's probability function for classification. An example of an SVM-XGB Classification Model hybrid is shown in Figure 1.

The Gradient Boosting Classifier model and the Support Vector Classifier model were combined to produce this new model to increase their accuracy. SVM-GBC classification model's mathematical formula is used as follows to classify objects:

TABLE 2 Features description.

Feature	Value	Description	Variable type
Meter ID	Integer Number	User and Consumer IDs	Input Variable
EMS	Integer Number	Monitoring System Protocol	Input Variable
MMS	Integer Number	Manufacturing Message Protocol	Input Variable
Data Flow Packets	Integer Number	Number Packets during a flow of message	Input Variable
Source Packets	Integer Number	Packets from source	Input Variable
Destination packets	Integer Number	Packets towards destination	Input Variable
IEDs	Integer Number	Intelligent electronic devices ID numbers	Input Variable
Attack	0 or 1	0 No attack occurs	Output variable
		1 FDI occurs	

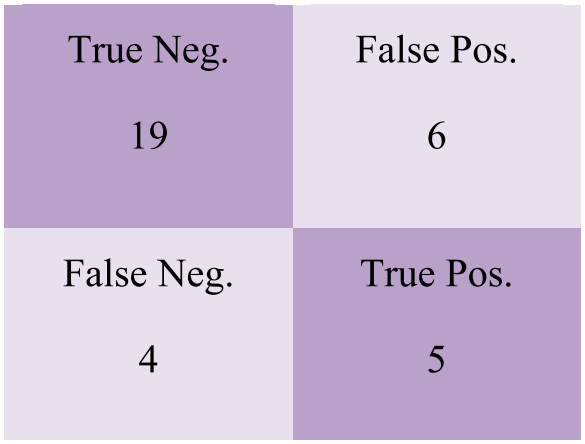

FIGURE 6
Classification model performance.the confusion matrix of SVM-XGB

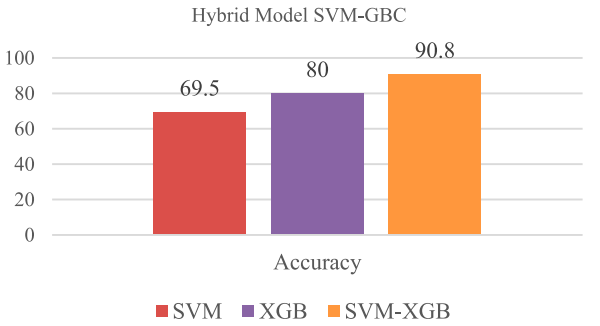

FIGURE 7
Classification Model.SVM-GBC classification model performance.

$$y = y^i = y^i + \alpha * \frac{\partial \sum (y_i - y_i^p)^2}{\partial y_p^i} \quad (6)$$

Then we will calculate the support vectors to classify FDI attacks in dataset as:

$$w.y + b = 1 \ldots (vector\ 1) \quad (7)$$

$$w.y + b = -1 \ldots (vector\ 2) \quad (8)$$

Support Vector Classifier probability function P, and GBC classification model output y^i are shown here. $\frac{\partial \sum (y_i - y_i^p)^2}{\partial y_p^i}$ Residual in trees and GBC's learning rate are seen in this graph. A Support Vector Classifier probability function will be used for classification if GBC receives the output of y. The SVM-GBC Classification Model hybrid is shown in Figure 1:

The Support Vector Classifier model was combined with the AdaBoost Classifier model in order to increase the accuracy of both models. The SVM-ABC Classification model's mathematical model is as follows:

$$y = significance \sum_{t=1}^{T} \alpha_t h_t(x) \ldots (a) \quad (9)$$

In order to classify FDI attacks in a dataset, we shall first calculate support vectors:

$$w.y + b = 1 \ldots (vector\ 1) \quad (10)$$

$$w.y + b = -1 \ldots (vector\ 2) \quad (11)$$

The support vector classifier's probability function is P, and the ABC classification model's output is y. $\sum_{t=1}^{T} \alpha_t h_t(x)$ It takes (x) hours to go to (t) in trees, it shows the sum of residuals. A Support Vector Classifier probability function is used to classify ABC's output of y. Figure 2 shows the SVM-ABC Classification Model hybrid model:

The Support Vector Classifier and CatBoost Classifier models were combined to improve the accuracy of both models, resulting in this model. SVM-CBC uses the following mathematical model to categories data:

The model will be initialized in the first stage,

$$F_o(x) = argmin_\gamma \sum_{i=1}^{n} L(y, y) \quad (12)$$

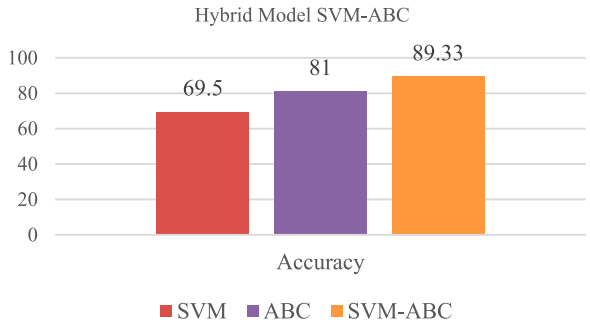

FIGURE 8
SVM-ABC classification model performance.

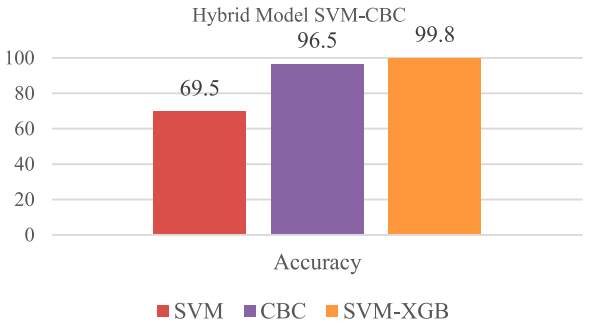

FIGURE 10
Classification Model.SVM-CBC

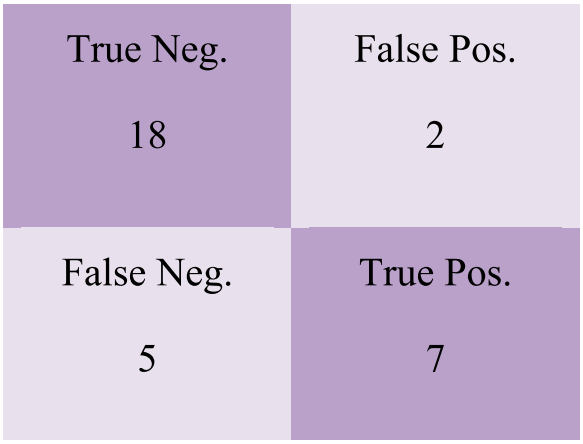

FIGURE 9
Confusion matrix of SVM-ABC Classification Model.

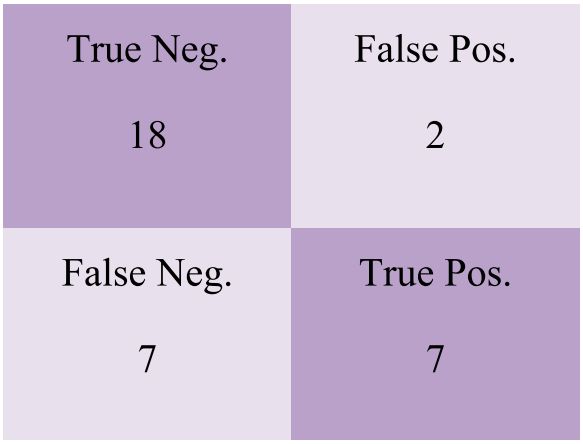

FIGURE 11
The confusion matrix of SVM-CBC

For m = 1 to M, we will compute the residuals.

$$\gamma_{im} = -\left[\frac{\partial L[y, F(x_i)]}{\partial F x_i}\right]_{F(x)=F_{M-1}(x)} \tag{13}$$

In order to compute the pseudo residuals, we will first fit the base leaner:

$$\gamma_{im} = argmin_{\gamma}\sum_{xi}^{n} L\left(y, F_{M-1}(x)\right) \tag{14}$$

Updated Model will be:

$$y = F_m(x) = F_{M-1}(x) + \alpha\sum_{i=1}^{n}\gamma_{im} \tag{15}$$

Classifying FDI attacks in a dataset will therefore require us to generate support vectors:

$$w.y + b = 1 \ldots (vector\ 1) \tag{16}$$

$$w.y + b = -1 \ldots (vector\ 2) \tag{17}$$

The Support Vector Classifier's probability function is P, and the CBC classification model's output is y. In other words, $[\frac{\partial L[y,F(x_i)]}{\partial F x_i}]_{F(x)=F_{M-1}(x)}$ the Mathematical expression: In the form of a tree, this function displays the total residual value. A Support Vector Classifier (SVC) probability function will be used to classify the CBC output of y when it is interpreted as a function of y and $argmin_{\gamma}\sum_{xi}^{n} L\left(y, F_{M-1}(x)\right)$. Figure 3 depicts the SVM-CBC Classification Model hybrid model:

The Support Vector Classifier model was combined with the Light-Gradient Boosting Model Classifier to improve the accuracy of both models. The following is the mathematical model for the SVM-LGBM Classification Model:

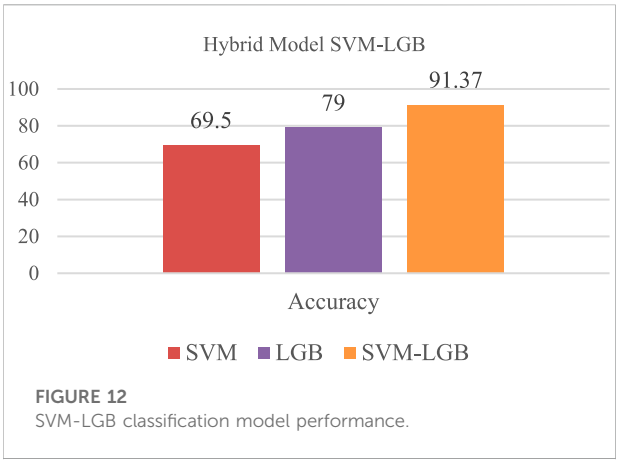

FIGURE 12
SVM-LGB classification model performance.

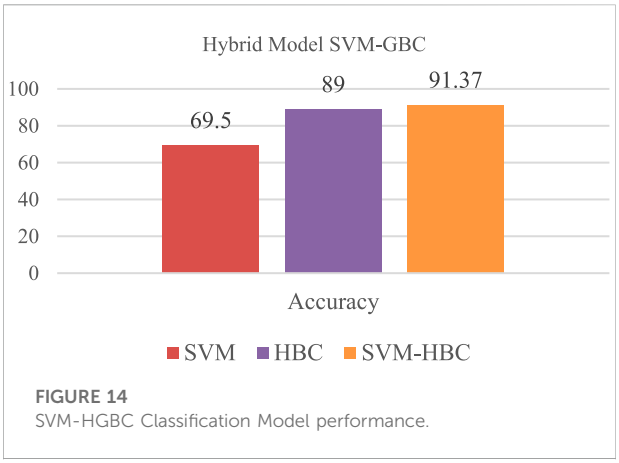

FIGURE 14
SVM-HGBC Classification Model performance.

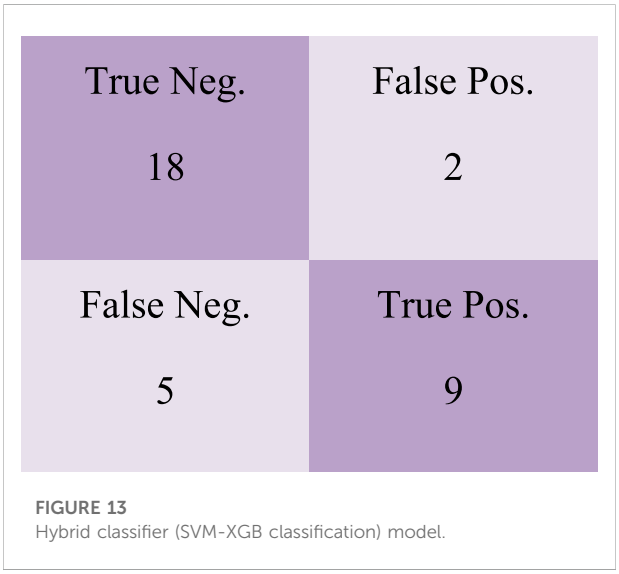

FIGURE 13
Hybrid classifier (SVM-XGB classification) model.

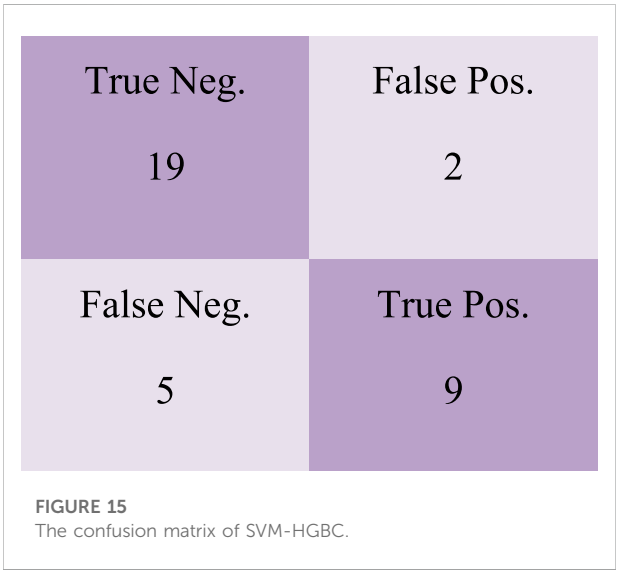

FIGURE 15
The confusion matrix of SVM-HGBC.

$$y = \alpha \sum_{t_i \epsilon Tree}^{T} \eta^i * leaf\,(t_i) \tag{18}$$

In order to classify FDI attacks in a dataset, we shall first calculate support vectors:

$$w.y + b = 1 \ldots (vector\ 1) \tag{19}$$

$$w.y + b = -1 \ldots (vector\ 2) \tag{20}$$

Support Vector Classifier probability function P, and LGBM classification model's output y are shown below. $\sum_{t_i \epsilon Tree}^{T} \eta^i * leaf\,(t_i)$ Learning rate is shown as a residual sum in the leaves. Support Vector Classifier is used to classify the output of LGBM when it receives the output of y. Figure 4 depicts the SVM-LGBM Classification Model hybrid:

SVG and HGBC have been merged to improve the accuracy of both models using support vector machines. Model of the SVM-HGBC Classification:

$$y = \frac{sum\ of\ residuals}{sum\ of\ each\,(1-p)\,for\ each\ sample\ in\ the\ leaf} \tag{21}$$

In order to classify FDI attacks in a dataset, we shall first calculate support vectors:

$$w.y + b = 1 \ldots (vector\ 1) \tag{22}$$

$$w.y + b = -1 \ldots (vector\ 2) \tag{23}$$

Support Vector Classifier probability function P and HGBC classification model's output y are shown in this equation. Every sample in the leaf is summed up to the sum of the residuals $\frac{sum\ of\ residuals}{sum\ of\ each\,(1-p)\,for\ each\ sample\ in\ the\ leaf}$. Calculates the total amount of waste in the form of a tree

TABLE 3 Description of metrics.

Metric	Description
Accuracy	Accuracy = $\frac{TP}{(TP+TN)*100}$
	True-Positive (TP): the feature result is 1 and sample is present in this data file
	True-Negative (TN): the feature result is 0 and sample is absent in data file
Confusion Matrix	

TABLE 4 Comparative Analysis for the detection of FDI.

Model	Accuracy (%)
SVM-XGB	95.50
SVM-GBC	90.80
SVM-ABC	89.33
SVM-CBC	99.80
SVM-LGBM	91.37
Logi HGBC	91.37

diagram. When HGBC receives the value of y, it passes it on to the support vector classifier's probability function for classification. As depicted in Figure 5 is a hybrid model of the SVM-HGBC Classification Model:

3.1.8 Performance Parameters

The system's accuracy has been evaluated using the F1 Score and accuracy measurements. The classification and misclassification clauses have been classed and misclassified, according to the confusion matrix. Table 2 displays the metrics that were used in this study.

4 Results

4.1 Hybrid model SVM-XGB

The XGBoost Classifier has been used to integrate these two models in order to improve their accuracy even further. Data from y will be fed into XGB's logistic regression probability function. The hybrid classifier improved accuracy from 89.5% to 95.5 percent in 69.5 percent of the time, according to an independent analysis using Logistic Regression. Model Performance of SVM-XGB Classification Models is shown in Figure 6.

For the SVM-XGB Classification Model, the confusion matrix is depicted in Figure 7 with a total of 19 True Negative and 2 True Positive values.

4.2 Hybrid model SVM-GBC

Using a combination of logistic regression and gradient boosting classifier approaches, this model was developed to improve both models' accuracy even further. After receiving y's output from the GBC. As can be seen in the graph below,

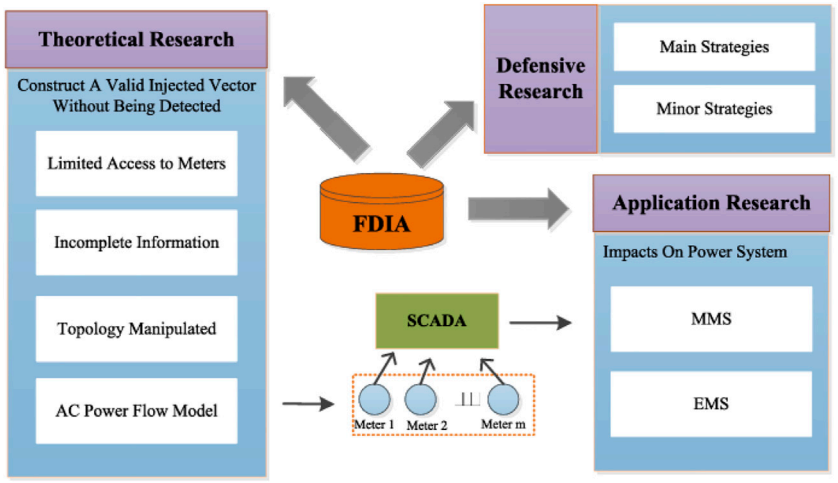

FIGURE 16
False data injection protection system.

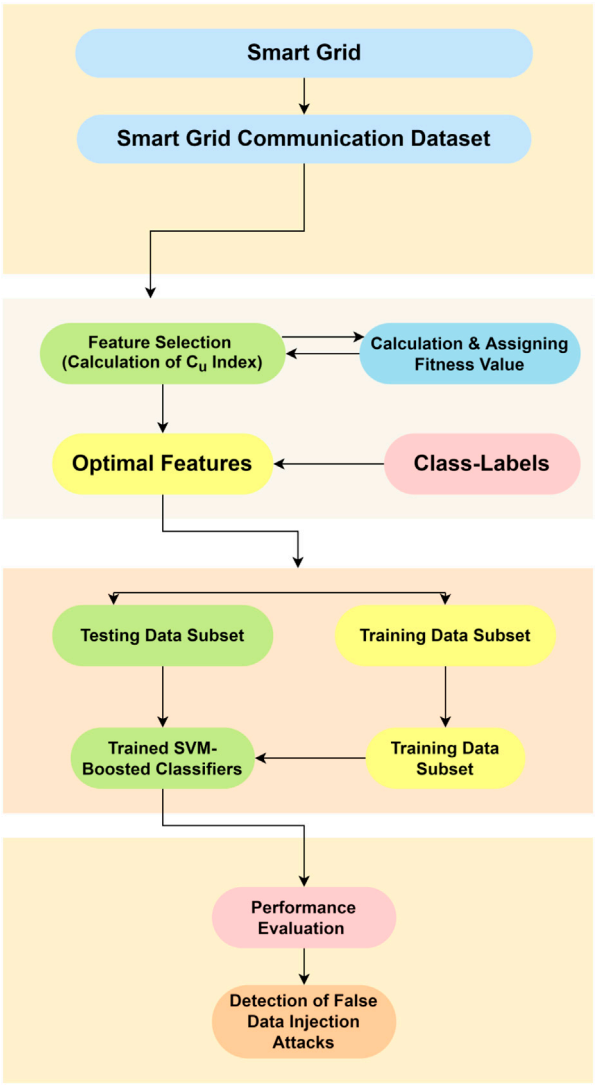

FIGURE 17
Proposed Workflow.

the SVM-GBC Classification Model hybrid model performed quite well, with an accuracy rate of 90.8%.

On the confusion matrix shown in Figure 8, there are 18 True Negative values, two False Positive values, nine False Negative values and seven True Positive values.

4.3 Hybrid model SVM-ABC

The logistic regression model's accuracy was improved by combining AdaBoost Classifier with it. It's subjected to a logistic regression to see how likely it is. Figure 9 shows the hybrid SVM-ABC Classification Model Performance model with an accuracy rate of 89.33 percent.

As shown in Figure 10, there are 19 True Negative values in the SVM-ABC Classification Model (SVM-ABC Classification Model) and 8 True Positive values.

4.4 Hybrid model SVM- CBC

With the use of the CatBoost Classifier and a logistic regression model, both models were improved in accuracy. If it is received from the CBC in the form of L (y, F (M-1) (x)), it will be supplied to the logistic regression's probability function for classification. As of this writing, SVM-CBC was the most accurate, with a 99.80% success rate. The SVM-CBC Classification Model is shown in Figure 11 as a hybrid model.

It is shown in Figure 12 that the SVM-CBC Classification Model has a confusion matrix with a total of 19 True Negative and 2 True Positive values.

4.5 Hybrid model SVM- LGB

It's possible to improve on both models by mixing them. The probability function of logistic regression will then be used by the LGBM to classify the attacks. As shown in Figure 13, the hybrid SVM-LGBM Classification Model is 91.37% accurate:

False Positive, False Negative, and True Positive values are shown in the confusion matrix of the SVM-LGB Classification Model in Figure 14.

4.6 Hybrid model SVM- HBC

With the help of the Histogram Gradient Boosting Classifier and the logistic regression model, it was created. The probability function of logistic regression will be analyzed as soon as it is received by HGBC to see if a class has been reclassified. Figure 15 shows the accuracy of the hybrid model at 91.37 percent:

Figure 20 depicts the SVM-HGBC Classification Model's confusion matrix, which includes 19 True Negative, 2 False Positive, 9 False Negative, and 3 True Positive values.

4.7 Comparative analysis

The accuracy percentages for several models are shown in the table below. SVM-XGB had a 95.5 percent accuracy rating, whereas SVM-GBC had a 90.8 percent accuracy rating. SVM-ABC, on the other hand, achieved an accuracy rate of 89.33 percent. SVM-CBC has the highest Accuracy of 99.80%. With a combined accuracy of 91.37 percent, the SVM-LGBM and the SVM-HGBC were used to test this hypothesis. When compared to other Logitboosted Algorithms used in previous

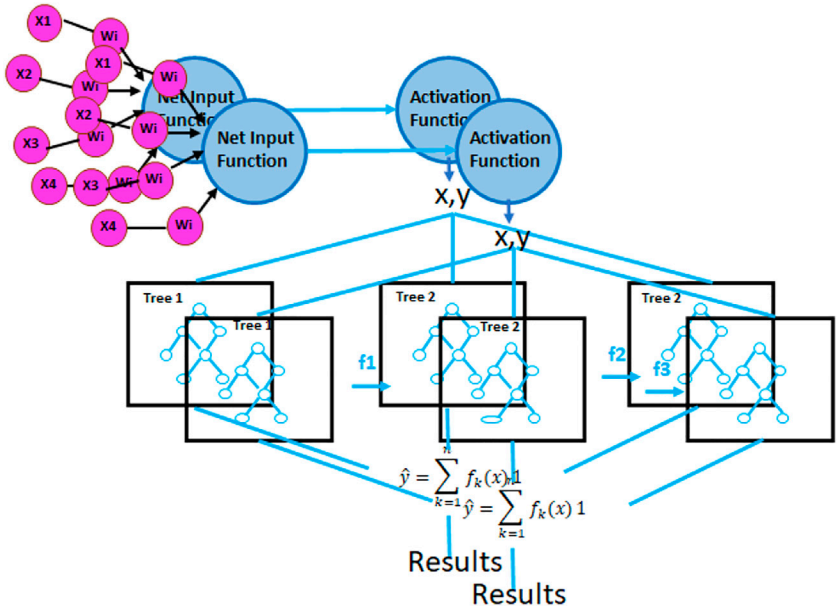

FIGURE 18
The confusion matrix of SVM-LBC Classification Model.

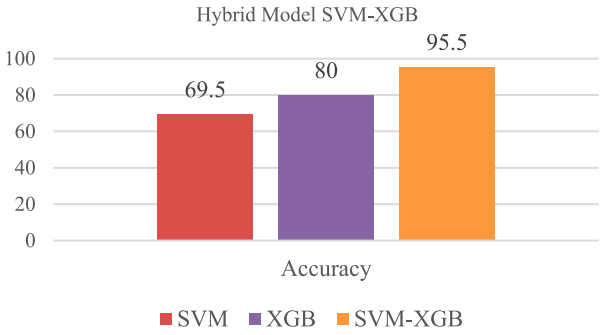

FIGURE 19
Hybrid Model SVM-XGB. SVM-XGB Classification Model Performance is shown in Figure 10.

FIGURE 20
The confusion matrix of SVM-GBC Classification Model.

studies on the given dataset, our proposed SVM-CBC has the highest accuracy. Table 3 shows a comparison of the proposed models: (Table 4).

5 Conclusion

The most common sort of cyber-attack against smart grids is False Data Injection (FDI). Because of the limitations of current bad data detection methods, it is currently impossible to detect covert FDI attacks. FDI (foreign direct investment) dangers can be detected using a variety of methods, including machine learning. An SVM-boosting algorithm-based study analyses six distinct supervised learning hybrid strategies that can be employed with six different boosted and feature selection (FS) approaches. Using a smart grid dataset, different solutions are evaluated. For each detection

approach, the classification accuracy is employed as a primary measure of performance. Using supervised learning and hybrid methodologies, it was discovered that the classification algorithms for FDI attack detection improved. The real-time smart grid datasets that can be used to execute these strategies make them interesting for future work in optimization and feature selection (Figure 16, Figure 17, Figure 18, Figure 19, Figure 20).

According to the authors, no financial or commercial affiliations were involved in the research, which could be seen as potentially conflicting.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

SA, MI, and SH contributed to conception and design of the study. DD organized the database. MI performed the ML (Machine Learning analysis). Supervision, resources, project administration, and funding acquisition, JW. SA wrote the first draft of the manuscript. SA, JW, SA, SH, and MI wrote sections of the manuscript. All authors contributed to manuscript revision, read, and approved the submitted version.

Acknowledgments

This is a brief acknowledgement of the contributions of individual colleagues, institutions, or agencies that assisted the writers' efforts in the writing of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Abu Hussein, A., Hasan Ali, M., and Author, C. (2014). Comparison among series compensators for fault ride through capability enhancement of wind generator systems. *Int. J. Renew. energy Res.* 4 (3), 116–126. doi:10.1049/iet-rpg.2015.0055

Akram, A., Ren, J., Rizwan, T., Irshad, M., Noman, S. M., Arshad, J., et al. (2021). A pilot study on survivability of networking based on the mobile communication agents. *Int. J. Netw. Secur.* 23 (2), 220–228. doi:10.6633/IJNS.202103_23(2).04

Al-Sahaf, H., Bi, Y., Chen, Q., Lensen, A., Mei, Y., Sun, Y., et al. (2019). A survey on evolutionary machine learning. *J. R. Soc. N. Z.* 49 (2), 205–228. doi:10.1080/03036758.2019.1609052

Ashrafuzzaman, M., Das, S., Chakhchoukh, Y., Shiva, S., and Sheldon, F. T. (2020). Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning. *Comput. Secur.* 97, 101994. doi:10.1016/J.COSE.2020.101994

Aziz, S., Jiang, H., Peng, J.-C., Ruan, J.-Q., and Wang, H.-Z. (2017). "Optimization of base operation points of MTDC grid for improving transition smooth," in Proceeding of the 2017 IEEE Conf. Energy Internet Energy Syst. Integr. EI2 2017 - Proc., Jun 2017 (IEEE), 1–6. doi:10.1109/EI2.2017.8244406

Aziz, S., Faiz, M. T., Adeniyi, A. M., Loo, K.-H., Hasan, K. N., Xu, L., et al. (2022). Anomaly detection in the internet of vehicular networks using explainable neural networks (xNN). *Mathematics* 10, 1267. doi:10.3390/math10081267

Boudreaux, J. A., and Boudreaux, J. (2018). Design, simulation, and construction of an IEEE 14-bus power system," *LSU Master's Theses*, 4801, doi:10.31390/digitalcommons.lsu.edu/gradschool_theses/4801

Case, M. J., Johnson, B. G., Bartowitz, K. J., and Hudiburg, T. W. (2021). Forests of the future: Climate change impacts and implications for carbon storage in the Pacific Northwest, USA. *For. Ecol. Manag.* 482, 118886. doi:10.1016/J.FORECO.2020.118886

Chehri, A., Fofana, I., and Yang, X. (2021). Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability* 13, 3196. doi:10.3390/SU13063196

Fu, X. (2022). Statistical machine learning model for capacitor planning considering uncertainties in photovoltaic power. *Protection Control Mod. Power Syst.* V (1), 51–63. doi:10.1186/s41601-022-00228-z

Fu, X., Guo, Q., and Sun, H. (2020). Statistical machine learning model for stochastic optimal planning of distribution networks considering a dynamic correlation and dimension reduction. *IEEE Trans. Smart Grid* 11, 2904–2917. doi:10.1109/tsg.2020.2974021

Ge, R., Feng, G., Jing, X., Zhang, R., Wang, P., and Wu, Q. (2020). EnACP: An ensemble learning model for identification of anticancer peptides. *Front. Genet.* 11, 760. doi:10.3389/FGENE.2020.00760/BIBTEX

Hu, B., Noman, S. M., Irshad, M., Tang, X., Song, C., and Muhammad, M. U. (2021). Run-time prediction practices of multimedia web design in technology management. *Smart Innov. Syst. Technol.* 236, 179–186. doi:10.1007/978-981-16-3180-1_23/TABLES/1

Irshad, M., Liu, W., Wang, L., and Khalil, M. U. R. (2021). Cogent machine learning algorithm for indoor and underwater localization using visible light spectrum. *Wirel. Pers. Commun.* 116 (2), 993–1008. doi:10.1007/s11277-019-06631-4

Lee, C., Panda, P., Srinivasan, G., and Roy, K. (2018). Training deep spiking convolutional Neural Networks with STDP-based unsupervised pre-training followed by supervised fine-tuning. *Front. Neurosci.* 12 (AUG), 435. doi:10.3389/FNINS.2018.00435/BIBTEX

Li, Y., Xue, W., Wu, T., Wang, H., Zhou, B., Aziz, S., et al. (2021). Intrusion detection of cyber physical energy system based on multivariate ensemble classification. *Energy* 218, 119505. doi:10.1016/J.ENERGY.2020.119505

Long, H., Fu, X., Kong, W., Chen, H., Zhou, Y., and Yang, F. (2022). Key technologies and applications of rural energy internet in China. *Inf. Process. Agric.* (in press). doi:10.1016/j.inpa.2022.03.001

Ma, Z., Guo, S., Xu, G., and Aziz, S. (2020). Meta learning-based hybrid ensemble approach for short-term wind speed forecasting. *IEEE Access* 8, 172859–172868. doi:10.1109/ACCESS.2020.3025811

Majeed Butt, O., Zulqarnain, M., and Majeed Butt, T. (2021). Recent advancement in smart grid technology: Future prospects in the electrical power network. *Ain Shams Eng. J.* 12 (1), 687–695. doi:10.1016/J.ASEJ.2020.05.004

Moghadam, M. F., Mohajerzdeh, A., Karimipour, H., Chitsaz, H., Karimi, R., and Molavi, B. (2020). A privacy protection key agreement protocol based on ECC for smart grid. *Handb. Big Data Priv.*, 63–76. doi:10.1007/978-3-030-38557-6_4/TABLES/3

Mohammadi Rouzbahani, H., Grids, S., Rouzbahani, H. M., Karimipour, H., and Lei, L. (2022). Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids. *Tech. Rxiv*, 0–10. doi:10.36227/techrxiv.19398449.v1

Mollah, M. B., Zhao, J., Niyato, D., Lam, K.-Y., Zhang, X., Ghias, A. M. Y. M., et al. (2021). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* 8 (1), 18–43. doi:10.1109/JIOT.2020.2993601

Murthy, A., Irshad, M., Noman, S. M., Tang, X., Hu, B., Chen, S., et al. (2022). Internet of Things, a vision of digital twins and case studies. *IoT Spacecr. Inf.*, 101–127. doi:10.1016/B978-0-12-821051-2.00010-6

Qi, R., Rasband, C., Zheng, J., and Longoria, R. (2021). Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning. *Information* 12, 328. doi:10.3390/INFO12080328

Qu, Z., Dong, Y., Qu, N., Li, H., Cui, M., Bo, X., et al. (2021). False data injection attack detection in power systems based on cyber-physical attack genes. *Front. Energy Res.* 9, 57. doi:10.3389/FENRG.2021.644489/BIBTEX

Rajendran, G., Sathyabalu, H. V., Sachi, M., and Devarajan, V. (2019). "Cyber security in smart grid: Challenges and solutions," in Proceeding of the 2019 2nd Int. Conf. Power Embed. Drive Control. ICPEDC, Chennai, India, August 2019 (IEEE), 546–551. doi:10.1109/ICPEDC47771.2019.9036484

Ruan, J.-q., Wang, H.-z., Liu, Y.-t., Aziz, S., Peng, J.-c., and Wang, G.-b. (2017). "AC sparse modeling for false data injection attack on smart gird," in Proceeding of the 2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT), Singapore, 2017 October (IEEE), 1–5. doi:10.1109/ACEPT.2017.8168567

Ruan, J., Liang, G., Zhao, J., Qiu, J., and Dong, Z. Y. (2022). An inertia-based data recovery scheme for false data injection attack. *IEEE Trans. Ind. Inf.*, 1. doi:10.1109/TII.2022.3146859

Sakhnini, J., Karimipour, H., and Dehghantanha, A. (2019). "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in Proceeding of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering SEGE, Oshawa, ON, Canada, Aug 2019 (IEEE), 108–112. doi:10.1109/SEGE.2019.8859946

Sami, M., Khan, S. Q., Khurram, M., Farooq, M. U., Anjum, R., Aziz, S., et al. (2022). A deep learning-based sensor modeling for smart irrigation system. *Agronomy* 12, 212. doi:10.3390/AGRONOMY12010212

Sargolzaei, A., Yazdani, K., Abbaspour, A., Crane, C. D., and Dixon, W. E. (2020). Detection and mitigation of false data injection attacks in networked control systems. *IEEE Trans. Ind. Inf.* 16 (6), 4281–4292. doi:10.1109/TII.2019.2952067

Sayghe, A., Hu, Y., Zografopoulos, I., Liu, X., Dutta, R. G., Jin, Y., et al. (2020). Survey of machine learning methods for detecting false data injection attacks in power systems. *IET Smart Grid* 3 (5), 581–595. doi:10.1049/IET-STG.2020.0015

Sengan, S., Subramaniyaswamy, V., Indragandhi, V., Velayutham, P., and Ravi, L. (2021). Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. *Comput. Electr. Eng.* 93 (September 2021), 107211. doi:10.1016/j.compeleceng.2021.107211

Sundar, K., Ashar, N., and Qinzhou, L. (2021). *IoT network attack detection using supervised machine learning*. [Online]. Available: https://shsu-ir.tdl.org/handle/20.500.11875/3245 (Accessed May 28, 2022).

Tan, L., Tong, Z., Kaifang, Z., Liang, Z., and Li, Z. (2017). "Fault division method of multi-infeed HVDC tranmission system based on fault current limiting technology," in Proceeding of the 2017 Chinese Automation Congress (CAC), Jinan, China, 2017 October (IEEE), 5668–5672. doi:10.1109/CAC.2017.8243794

Tarafdar Hagh, M., Muttaqi, K. M., Sutanto, D., Hossain, M. S. A., and Haidar, A. M. A. (2015). Improving fault ride-through capability of DFIG based wind generators by using bridge-type superconducting fault current limiter. *Proc. Univ. Power Eng. Conf.* 2015 (c), 2–6. doi:10.1109/UPEC.2015.7339856

Triantafyllou, A., Sarigiannidis, P., and Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends. *Wirel. Commun. Mob. Comput.* 2018, 1–24. doi:10.1155/2018/5349894

Wang, H., Cai, R., Zhou, B., Aziz, S., Qin, B., Voropai, N., et al. (2020). Solar irradiance forecasting based on direct explainable neural network. *Energy Convers. Manag.* 226, 113487. doi:10.1016/J.ENCONMAN.2020.113487

Wilson, D., Tang, Y., Yan, J., and Lu, Z. (2018). "Deep learning-aided cyber-attack detection in power transmission systems," in Proceeding of the 2018 IEEE Power & Energy Society General Meeting (PESGM), OR, USA, August 2018 (IEEE). doi:10.1109/PESGM.2018.8586334

Wu, J., Haider, S. A., Irshad, M., Arshad, J., Noman, S. M., Murthy, A., et al. (2021). Li-pos: A light positioning framework leveraging ofdm for visible light communication. *Sensors* 21, 4310. doi:10.3390/S21134310

Yang, W., Wang, M., Aziz, S., and Kharal, A. Y. (2020). Magnitude-reshaping strategy for harmonic suppression of VSG-based inverter under weak grid. *IEEE Access* 8, 184399–184413. doi:10.1109/ACCESS.2020.3026054

Ye, L., and Lin, L. Z. (2010). Study of superconducting fault current limiters for system integration of wind farms. *IEEE Trans. Appl. Supercond.* 20 (3), 1233–1237. doi:10.1109/TASC.2009.2039469