IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 31 May 2024, accepted 24 July 2024, date of publication 29 July 2024, date of current version 7 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3435564

RESEARCH ARTICLE

An Edge Computing-Based and Threat Behavior-Aware Smart Prioritization Framework for Cybersecurity Intrusion Detection and Prevention of IEDs in Smart Grids With Integration of Modified LGBM and One Class-SVM Models

ABDULMOHSEN ALGARNI[1], ZULFIQAR AHMAD[2], AND MOHAMMED ALAA ALA'ANZY[3]
[1]Department of Computer Science, King Khalid University, Abha 61421, Saudi Arabia
[2]Department of Computer Science and Information Technology, Hazara University, Mansehra 21300, Pakistan
[3]Department of Computer Science, SDU University, 040900 Almaty, Kazakhstan

Corresponding authors: Zulfiqar Ahmad (zulfiqarahmad@hu.edu.pk) and Mohammed Alaa Ala'anzy (m.alanzy.cs@gmail.com)

This work was supported by the Deanship of Scientific Research at King Khalid University under Grant R.G.P.2/93/45.

ABSTRACT The smart grid environment, which emphasizes sustainability, dependability, and efficiency through smart components such as Intelligent Electronic Devices (IEDs), communication networks, and control systems, marks a revolutionary change in the way traditional power distribution is carried out. As smart grids grow and are integrated into energy distribution networks, these systems become more vulnerable to cybersecurity threats due to their increased connectivity, usage of IEDs, and reliance on digital communication channels. This study presents an edge computing-based, threat behavior-aware smart prioritization framework with binary and multidimensional classification and detection of cybersecurity intrusions through modified machine learning methods. The proposed framework has the potential to improve smart grid cybersecurity by offering a comprehensive defense against intrusion threats. The proposed framework enhances smart grid cybersecurity by utilizing a multi-criteria approach. It implements edge-computing technology for data storage and processing in smart grids. It applies machine-learning models for cybersecurity intrusion detection in IEDs and provides prevention by assigning priorities to the threats based on their behavior. In order to show the effectiveness of the proposed framework, we modified and implemented two machine-learning models, i.e., LGBM and One Class-SVM, as proposed models in the framework. For multidimensional classification and detection of cybersecurity intrusions in IEDs of smart grids, we used LGBM. Whereas, for binary classification and detection of cybersecurity intrusions, we used One Class-SVM. We simulated the detection and classification of cybersecurity intrusions in IEDs using a power system intrusion dataset. The results show that the LGBM model provides an accuracy of 93%, precision of 94%, recall of 93%, and F1 score of 93% in the detection and classification of cybersecurity intrusions in IEDs of smart grids. The implementation of One Class-SVM with binary classification yields an accuracy of 85%, precision of 89%, recall of 85%, and F1 score of 86%. We implemented the benchmark machine-learning models, i.e., Gradient Boosting Machine and Support Vector Machine, for performance comparison with the proposed modified machine-learning models. The performance comparison shows that

The associate editor coordinating the review of this manuscript and approving it for publication was Enamul Haque.

the modified machine learning models implemented in the proposed framework outperformed the benchmark machine-learning models.

INDEX TERMS Smart grids, cyberattack detection and prevention, IEDs, LGBM, One Class-SVM, intrusions.

I. INTRODUCTION

The ''smart grid environment'' is a paradigm shift in the conventional electrical supply network that produces a more sustainable, dependable, and efficient electrical infrastructure [1]. In order to maximize the production, distribution, and consumption of electricity, this updated grid includes a variety of innovative components, such as intelligent electronic devices (IEDs), communication networks, control systems, and data analytics tools [2]. The smart grids focus on information and communication technology in the operation. Smart meters, as an example of IEDs, have a huge role to play by providing detailed information on energy usage. Smart meters enable the provision of communication from the utility providers to the customers and vice versa in an efficient manner to enhance the control of power usage. Another part of the smart grid is the connectivity of communication networks and sensors [3]. In order to gather information on several characteristics including voltage, current, and power quality, these sensors are placed throughout the grid. The grids communication networks enable information sharing amongst its various components, facilitating prompt reactions to changing circumstances and enhancing overall grid reliability. One important feature of the smart grid is automation, which is made possible by sophisticated control systems [4]. These systems automate the grids that are operating in real-time by employing AI and data analytics. For example, they can better manage production and consumption, manage power distribution in case of an outage, and incorporate renewable energy into the grid seamlessly. The smart grid puts a lot of emphasis on the use of renewable energy. Managing these intermittent energy sources is made easier by the smart grid that is being adopted with the increased use of solar panels, wind turbines, and other distributed energy resources (DERs). Batteries and other energy storage devices are integrated into the grid to provide an additional source of energy during periods of low demand and to discharge it during periods of high demand [5], [6].

Smart grid ecosystems rely greatly on IEDs for their evolution and functionality [7]. The embedded intelligence, communication capabilities, and function-specific aptitude are the important characteristics of these devices inside the larger smart grid infrastructure. IEDs are widely used in the smart grid to measure and monitor a variety of characteristics. This entails keeping an eye on power quality, voltage levels, current flows, and other critical parameters [8]. Common examples of IEDs are smart meters, which give users access to real-time data on energy consumption at the consumer level [9]. This information helps utility companies and consumers make educated decisions. IEDs also play a major role in smart grids automation. These devices allow for automated reactions to changing grid conditions. For example, IEDs can rapidly isolate the impacted region, reroute power, and restore service without the need for human intervention in the event of a breakdown or outage. This lowers downtime and increases the resilience of the grid. IEDs have communication capabilities in order to facilitate smooth data interchange within the smart grid. These gadgets are in communication with utility operators, with central control systems. Decision-making, coordination, and grid operation optimization have been done in real time [10]. IEDs make it easier to integrate and manage distributed energy resources, such as solar and wind power, which are becoming more and more common in smart grids. They facilitate the seamless integration of clean energy into the grid, improve power flow, and assist balance the fluctuation of renewable supply [11].

Unauthorized access, manipulation, or disruption of the infrastructure's components and communication within a smart grid is referred to as an intrusion attack [12]. The smart grids operation, security, and dependability are seriously threatened by these attacks. The penetration in smart grids by these attacks include denial-of-service (DoS), unauthorized access, data manipulation and ransomware [13], [14]. DoS is referred to as putting too much strain on the control or communication networks of the smart grid to prevent regular operations. Unauthorized access means entering the smart grid infrastructure without authorization, thereby jeopardizing control systems or private information. Data manipulation is represented by changing or fabricating data in the smart grid, which could cause erroneous decisions to be made and jeopardize the system integrity. The introduction of ransomware or malicious software into the smart grid can result in extortion attempts, data breaches, and system outages. The target components of these attacks in a smart grid environment include IEDs, communication networks, and control systems [15].

In order to improve the cybersecurity of smart grid infrastructure machine learning techniques have been implemented [16], [17], [18], [19], [20], [21], [22]. This approach is especially effective when combined with a new processing and storage technology i.e., edge computing [23], [24], [25], [26], [27]. Machine learning techniques have the ability to identify typical behavior patterns in the smart grid [13], [15], [28], [29], [30], [31]. Labeled datasets including instances of both benign and malignant conduct can be used to train machine-learning algorithms. Guided learning techniques such as Support Vector Machines (SVMs) [32] is useful in intrusion detection. Edge computing reduces latency by processing data closer to the source. Edge computing allows real-time data analysis, facilitating quick detection and response to possible intrusions without depending on

centralized processing. To lessen the reliance on a single point of failure, edge computing divides computational duties among devices in the smart grid. Pre-trained models for intrusion detection have the ability to be installed on edge devices to facilitate local decision-making [16]. This is especially helpful in situations where quick response is needed to decrease the effects of an intrusion. Edge devices that have been trained to detect intrusions analyze data locally without transferring it to a central server by immediately deploying the models onto the devices.

A. RESEARCH MOTIVATION

The requirement of safeguarding advanced electrical infrastructure is the motivation behind creating a smart prioritizing framework for intrusion detection and prevention of IEDs inside a smart grid environment [2], [7], [8], [33]. As smart grids become more integrated into the energy distribution systems, these systems become more exposed to cybersecurity threats because of the high connectivity, use of IEDs, and reliance on digital communication. Smart grids are vulnerable to infiltration attacks, and their consequences range from power outages, alteration of data, and potential risks to public safety [34]. It is important that these vulnerabilities be addressed with creative and flexible security solutions. Given the real-time nature of smart grid operations, the proposed framework's integration of edge computing, behavior-aware techniques, and modified machine-learning methods intended to improve the effectiveness and responsiveness of intrusion detection. The proposed research aims to strengthen smart grid environment cybersecurity defenses with insightful observations and useful solutions, guaranteeing the ongoing dependability and resilience of our changing energy infrastructure against new cyber-threats.

B. MAIN CONTRIBUTIONS

There are following main contributions of the proposed research work:

- The study proposes a framework to enhance the cybersecurity of IEDs in smart grids by utilizing a multi-criteria approach. The proposed framework integrates edge-computing technology, modified machine-learning models and a threat behavior-aware approach to offer an enhanced protection mechanism against cybersecurity intrusion attacks on IEDs.
- The framework incorporates edge computing as a major advancement in real-time intrusion detection. The research addresses the need for quick and independent decision-making, lowering the response time to any threats within the dynamic and networked smart grid landscape, by processing data locally at the edge devices.
- A smart prioritization mechanism has been added to the proposed framework to rank the sensitivity of intrusions found, allowing resources to be allocated more effectively and security incidents to be handled more quickly.
- A holistic approach to cybersecurity in smart grids is proposed by the integration of intrusion behavior-aware approache, machine learning, and edge computing under a unified framework. Taking into consideration the complexities of the interconnected systems in a smart grid, this comprehensive method aims to provide a multi-faceted defense against intrusion threats.

C. ORGANIZATION OF THE PAPER

The rest of the paper is organized as follows: Section II presents the related work in connection with smart grid environments, IEDs, machine-learning techniques used for cybersecurity intrusion detection, and the use of edge computing in data processing and analysis. Section III presents the system design and model with an explanation of the various components of the proposed framework. Section IV provides an edge computing-based preventive framework for cybersecurity intrusion detection in smart grids with pseudocode. Section V presents the performance evaluation methodology. Section V provides experiments, results, and discussions. Section VI concludes the article with future directions.

II. RELATED WORK

The related work has been studied in connection with smart grid environments, machine learning techniques used for cybersecurity intrusion detection and use of edge computing in data processing and analysis.

Advanced Smart Grid (SG) ecosystems has been made possible by the prominence of the SG-to-Cloud continuum. Legacy Intelligent Electron Devices (IEDs) has been considered while designing future Smart Grid ecosystems. As a result, their complete integration into the Internet of Smart Grid Things (IoSGT) is a constant challenge. The authors in [33] presented the old Smart Grid to IoT Integration Approach (SG2IoT) to address this difficulty. This approach automates the integration of numerous old IEDs in a scalable and adaptable environment, made feasible by the IoSGT. In addition, a SG-to-Cloud continuum is established by the SG2IoT to provide architectural modular components for distributed operation at cloud facilities dispersed throughout edge and central datacenters. The SG2IoT effect estimation involved using a prototype that was operating on a testbed located in a lab that included real-world technologies. The SG2IoT lightweight approach feasibility is demonstrated by outcome analysis, which establishes an SG-to-Cloud continuum to enable quick response times and reasonably priced IoSGT scalability [33].

Smart grids have greatly reduced the contingencies of distribution networks and helped in their operation, control, and, most importantly, protection. The first phase of integrating smart grid switching devices into distribution networks is covered in [2]. At this point, conventional protection components (like fuses, reclosers, and sectionalizers) must be used with smart grid technologies. Due to the two different ideologies, this fact may present issues for the protection methods. In certain businesses, particularly those with modest

resources, these two protection concepts can coexist for a long time. The most widely used IEDs on the market are examined to confirm their features and see whether methods may be added to enable the two ideologies to coexist. The suggested method then demonstrates how the current IEDs can communicate with the conventional equipment. The suggested method converts the IEDs into intelligent agents. The effectiveness of the suggested methodology is demonstrated through the presentation and discussion of real-world examples utilizing distribution networks [2].

Many security concerns are currently ravishing Internet of Things (IoT) systems and harming information as a result of recent advancements in wireless communication that have led to a surge in IoT systems. Given the wide range of applications for IoT devices, it is important to make sure that hacks are comprehensively identified to prevent damage [35]. Algorithms for machine learning (ML) have shown a high capacity to reasonably accurately assist in mitigating assaults on IoT devices and other edge systems. One of the problems with IoT systems is that the dynamics of how hackers operate in IoT networks necessitate more advanced intrusion detection systems (IDS) models that can identify numerous attacks with a greater detection rate and less computational resource requirement. To propose IDS models for IoT contexts, a variety of ensemble methods have been applied with various ML classifiers, such as decision trees and random forests. One method for creating an ensemble classifier is the boosting method. Based on boosted ML classifiers, the research in [35] suggests an effective technique for identifying network breaches and cyberattacks. The authors proposed BoostedEnML as their model. First, they train one ensemble with a majority voting strategy and another using the stacking method on six different machine-learning classifiers (DT, RF, ET, LGBM, AD, and XGB). The IDS model was trained, assessed, and tested using two distinct datasets that contained well-known assaults, such as botnets, infiltration, web attacks, distributed denial of service (DDoS), denial of service (DoS), heartbleed, portscan, and botnets. The authors build their proposed BoostedEnsML model utilizing LightGBM and XGBoost based on the top two models because the two classifiers together produce a lightweight yet effective model, which is one of the goals of this study. According to experimental results, using the chosen datasets for multiclass classification, BoostedEnsML performed better than previous ensemble models in terms of accuracy, precision, recall, F-score, and area under the curve (AUC).

The necessity for cybersecurity has grown in importance over the past few years due to the quick development of network technologies. An intrusion detection system (IDS) is supposed to serve as the key defense mechanism, adapting to the ever-changing complex threat landscape and safeguarding computing infrastructures. Recently, a lot of deep learning algorithms have been developed [36]. However, because of network traffic imbalances and insufficient aberrant traffic samples for model training, these techniques have a hard time identifying all forms of assaults, especially infrequent ones. The unsupervised deep learning approach for intrusion detection presented in [36] aims to address these issues and enhance detection performance. This paper [36] introduces a novel single-stage IDS approach that integrates a one-dimensional convolutional autoencoder (1D CAE) and a one-class support vector machine (OCSVM) as a classifier into a joint optimization framework, in contrast to the current IDS model that extracts features and trains a classifier in two separate stages. By creating a unified objective function integrating reconstruction error and classification error, the technique simultaneously optimizes the 1D CAE for compact feature representation and the OC-SVM for classification using only the normal traffic samples.

The expansion of IoT into the industrial domain is known as Industrial IoT, or IIoT. It seeks to enhance industrial sectors' operations by integrating embedded devices. That being said, IIoT security flaws are more dangerous than IoT ones. Intrusion detection systems (IDS) are therefore designed to stop some extremely dangerous incursions. IDS keeps an eye on the surroundings to quickly identify intrusions. The research in [37] develops a machine learning-based intrusion detection method for IIoT security. The machine learning models' detection rate and accuracy (ACC) are enhanced by the feature selection and dimensionality reduction techniques. In order to mitigate the high complexity of the dataset, the authors suggest utilizing isolation forest (IF) and Pearson's correlation coefficient (PCC). Outliers are eliminated using the IF, and the feature selection procedure is carried out using the PCC [37]. The authors examined the effect of our suggested model on the unbalanced dataset known as the Bot-IoT using the Matthews correlation coefficient (MCC). To improve IDS performance, the RF classifier is used. Findings show that, in comparison to other models, the suggested strategy performs better and has several advantages.

The authors in [38] provide a thorough analysis of recent research efforts aimed at identifying and preventing attacks that take advantage of IEC-61850 substations. Their primary contribution is a unique taxonomy that includes elements of both design and evaluation for IDSs that are specific to substations. IDS architectures, detection techniques, analysis, actions, data sources, detection range, validation strategies, and metrics are all included in this taxonomy. They also provide an overview of the detection rules used by the most advanced intrusion detection systems and evaluate how resistant they are to five different kinds of attacks. Their analysis shows that while some attacks are addressed by IDSs that are currently in use, more development is especially required to address masquerade attacks.

The work in [39] presents a hybrid deep learning model that is semi-supervised and combines several anomaly detection algorithms (such as Isolation Forest, Local Outlier Factor, One-Class SVM, and Elliptical Envelope) with a Gated Recurrent Unit (GRU)-based Stacked Autoencoder (AE-GRU). In order to effectively capture temporal pat-

terns and dependencies, GRU units are used in both the encoder and decoder sides of the stacked autoencoder. This facilitates dimensionality reduction, feature extraction, and precise reconstruction for improved anomaly detection in smart grids. The suggested method makes use of unlabeled data to track network activity and spot erroneous data flows. In particular, the anomaly algorithms are used to identify possible cyberattacks after the AE-GRU is used to reduce the amount of data and extract pertinent features. The authors assess the suggested framework with the commonly used IEC 60870-5-104 traffic dataset.

In [40] paper, the authors use the throughput of OT (operational technology) communication network traffic to propose a new graph-based forensic analysis approach for anomaly detection in power systems. It uses a hybrid deep learning model that combines a convolutional neural network with graph convolutional long short-term memory. The suggested approach helps SOC (Security Operations Center) with post-mortem and ongoing OT security monitoring. The suggested approach can locate cyberattacks on power grid OT networks, according to the results, with an AUC score higher than 75%.

In order to mitigate cyberattacks on the GOOSE message virtual LAN (VLAN), a non-observable strongly connected biography, the work in [41] presents a study on deception technology (decoys). By defining observable subgraphs in the VLAN, the deployment of defender decoys is proposed. With the defender acting as the leader, the defender-attacker interaction is modeled as a single-leader, single-follower game. Then, a bi-level optimization problem is formulated to determine the best decoy allocation for asset protection and attack detection. Defender resource allocation considers both the sequential and simultaneous allocation of detection and protection decoys. It is established that the defender-attacker game is in equilibrium. In the PSRC-I5 protection relay report, the model is demonstrated in a 3-IED VLAN, and performance is assessed in a 12-IED VLAN system. Based on the results comparisons, it was found that the proposed model is capable of mitigating attacks in the GOOSE VLAN.

The literature review reveals that smart grids are increasingly susceptible to cybersecurity attacks due to the rising number of connections, the use of IEDs, and the reliance on digital communication channels. Existing studies have not explored the complexities of integrating edge computing within the framework of smart grid cybersecurity. There is a lack of a thorough assessment of the potential of edge computing with modified machine-learning models to enhance cybersecurity and prevent IEDs in smart grids. Binary and multidimensional classifications of cybersecurity intrusions in IEDs have not been made previously with specifically selected and modified machine learning models. The existing intrusion detection system has not significantly focused on the behavior of the intrusions and has not taken preventive measures based on the behavior of the intrusions. The goal of the proposed study is to improve the cybersecurity defense of IEDs in smart grids with edge computing technology, modified machine-learning models, and a threat behavior-aware smart periodization approach.

III. SYSTEM DESIGN AND MODEL

This research work proposes an edge computing-based and threat behavior-aware smart prioritization framework with modified LGBM and One Class-SVM methods for cybersecurity intrusion detection and prevention of IEDs in a smart grid environment as shown in Figure 1. Information has been gathered from multiple smart grid sources. These sources include data from sensors, communication networks, and intelligent electronic devices (IEDs). To train and run the intrusion detection model, data includes system logs, network traffic patterns, and device activity. To provide a baseline of typical behavior inside the smart grid, the model makes use of threat behavior-aware approach.

The proposed approach makes use of edge computing to process data locally close to where it is generated or consumed. Locally, edge devices implanted in IEDs or communication nodes perform intrusion detection and preliminary analysis. As a result, less raw data needs to be transmitted in bulk to a centralized server, improving real-time processing and lowering latency. Modified machine learning methods i.e., LGBM and One-Class SVM models have been implemented for intrusion detection in the smart grid environment. Based on the seriousness and urgency of detected intrusions, the proposed model incorporates a smart prioritization structure that ranks alerts. The implementation of this prioritizing technique guarantees the effective allocation of resources and timely actions, particularly in cases of serious security incidents. The criticality of the impacted devices and the possible effects on the smart grid functionality has been taken into consideration during setting priorities. The following are the main components of the proposed framework.

A. SMART GRID ENVIRONMENT

A smart grid environment is a high-tech electrical infrastructure that optimizes electricity generation, delivery, and consumption. The integration of diverse components, including sensors, communication networks, IEDs, and advanced control systems, aims to improve the sustainability, dependability, and efficiency of energy distribution. The smart grid environment is aimed to optimize energy consumption. The smart grid energy optimization is mathematically represented by equation 1.

$$P_{optimized} = \sum_{i=1}^{n} P_i - \sum_{j=1}^{m} L_j \tag{1}$$

where, $P_{optimized}$ is the optimized power, P_i is the power generated by each source and L_j is the power loss at each transmission line.

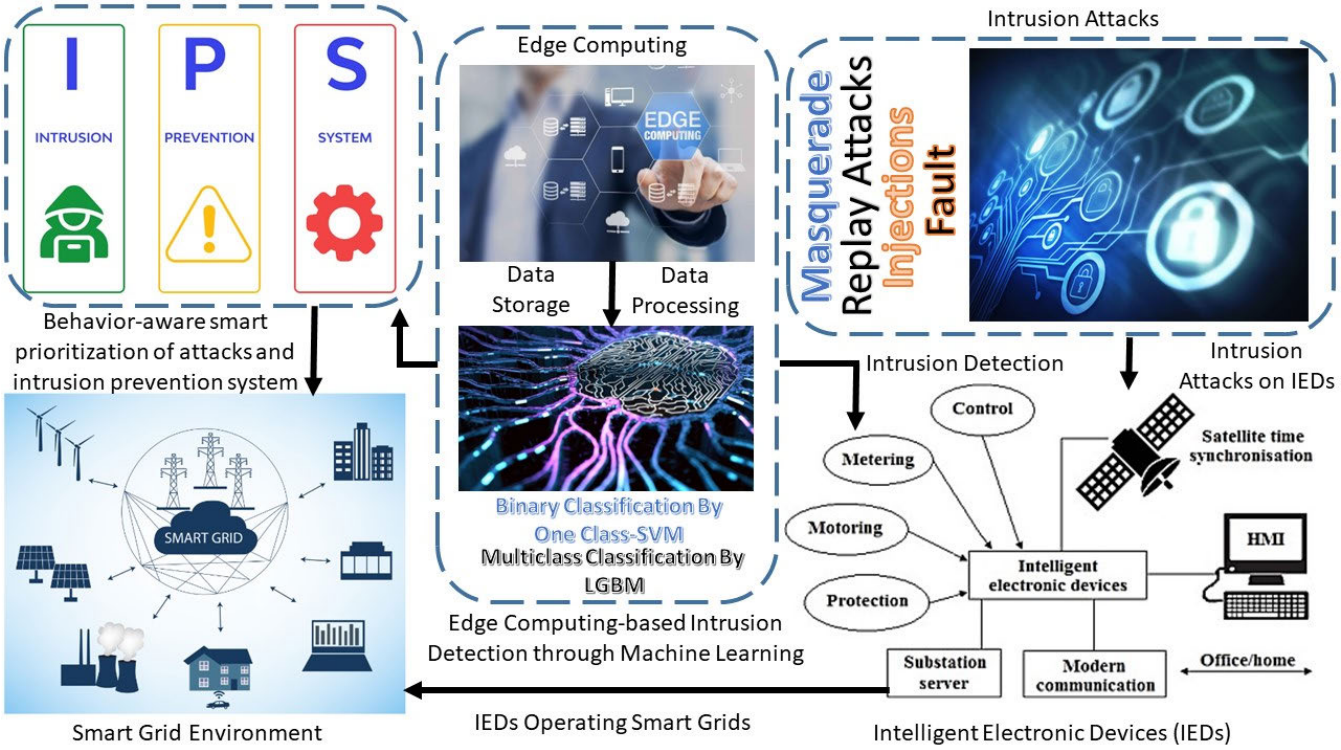


FIGURE 1. An edge computing-based and threat behavior-aware smart prioritization framework for cybersecurity intrusion detection in IEDs inside smart grid infrastructure.

The efficiency of the smart grid is mathematically represented by equation 2.

$$Efficiency = \frac{Useful\ power\ output}{Total\ power\ output} \times 100 \tag{2}$$

Smart grid infrastructure also incorporates renewable energy sources. The integration efficiency of renewable energy sources is mathematically represented by equation 3.

$$Integration\ Efficiency = \frac{Energy\ ouput\ from\ Renewable\ Sources}{Total\ Energy\ output} \times 100 \tag{3}$$

B. INTELLIGENT ELECTRONIC DEVICES (IEDS)

Intelligent Electronic Devices are essential parts of smart grid environment, serving as key components in applications related to protection, control, and monitoring [2], [7]. These components have communication features, embedded intelligence, and frequently have unique features like smart metering. IED integration is common in industries like power systems, where it improves operational safety, dependability, and efficiency. Functionality of protective relays of IEDs is mathematically represented by equation 4.

$$V_{out} = f\ (V_{in}, \theta_{in}, t) \tag{4}$$

where, V_{out} represents relay output, V_{in} is input voltage and θ_{in} is input phase angle. IEDs have capabilities to communicate with each other and to the base station or to the main grid station. The communication capability is measure by throughput and is given in equation 5.

$$Throughput = \frac{Data\ Size}{Transmission\ Time} \tag{5}$$

IEDs continuously gather data from the monitor system and have also been used for protection and control purposes. The protection mechanism is represented by equation 6.

$$Trip\ Decision = h\ (Measured\ Value, Thresholds) \tag{6}$$

IEDs are integrated in smart grid for monitoring and control purpose and mathematically represented by equation 7.

$$Integration\ Efficiency = \frac{Number\ of\ IEDs\ Integrted}{Total\ number\ of\ Devices} \times 100 \tag{7}$$

C. INTRUSION ATTACKS ON IEDS IN SMART GRID ENVIRONMENT

The implementation of the IEC-61850 standards for communication among Intelligent Electronic Devices (IEDs) presents new security issues in the domain of digital electrical substations in Smart Grids [42], [43]. Strong security measures are required for the implementation of these standards in order to protect the integrity and operation of digital substation services. The masquerade, replay attacks and injection attacks are the major cybersecurity threats that present unique difficulties in IEDs of smart grids.

Masquerade attacks are a kind of cybersecurity threat in which a hacker impersonates a trustworthy user or system component in order to obtain unauthorized access to a network or system. Impersonation or identity spoofing are alternative terms used to refer to these attacks. A masquerade threat attack on IEDs within smart grids has severe consequences. Masquerade attacks allow attackers to gain unauthorized control over IEDs, potentially leading to the manipulation of grid parameters including voltage levels, frequency, or power flow. If these attacks are not properly identified or there is no prevention mechanism, there is a probability of disruptions to the power supply or damage to connected devices. Equation 8 mathematically represents the probability of successful masquerade attacks.

$$P\,(Masquerade\ success) = \frac{Number\ of\ sucessful\ masqurade\ attempts}{Total\ number\ of\ attempts} \tag{8}$$

The analysis of the data concerning the behavior of devices can be used for identification of the signs that point at a masquerade attack. The preventive measures that can be taken are that the access controls should be strict, and privileges should be granted according to the roles and responsibilities of the users to prevent the masquerade attacks.

Replay attack is a type of cyberattack where the hacker intercepts the communication between two parties and then retransmits the messages back to the same parties. Replay attacks on IEDs within smart grids has dire consequences; it has severe impacts on the smart grid's electricity distribution system's integrity, reliability, and security. Replay attacks result in unauthorized access to the IEDs in the smart grid. The attackers could replay the captured messages or commands to take control of the devices like relays or switches and control the grid operations. The main threat that attackers can implement is the replay of legitimate data packets within the smart grid. This will lead to wrong measurement values, changed sensor data, or false status information, and thus wrong decisions of the grid management systems. Malicious replay attacks are capable of interfering with normal grid operations by feeding in wrong or out-of-date control signals. This will lead to unwanted operations, for instance, load shedding, wrong voltage corrections, or even failure progression, affecting the stability of the whole system. If attackers replay billing information or transactions, they will be able to manipulate billing systems or steal electricity, and it will be unnoticed. This could eventually reduce the income of the utility providers and, in turn, may also impact the consumers through wrong tariffs. Equation 9 mathematically represents the probability of successful replay attacks.

$$P\,(Replay\ success) = \frac{Number\ of\ sucessful\ replay\ attempts}{Total\ number\ of\ attempts} \tag{9}$$

In order to mitigate the risks of replay attacks, smart grid operations are required to implement robust security measures such as secure communication, authentication mechanisms and intrusion detection systems. Implementation of multi-factor authentication adds an extra layer of security beyond simple data transmission, making replay attacks more challenging.

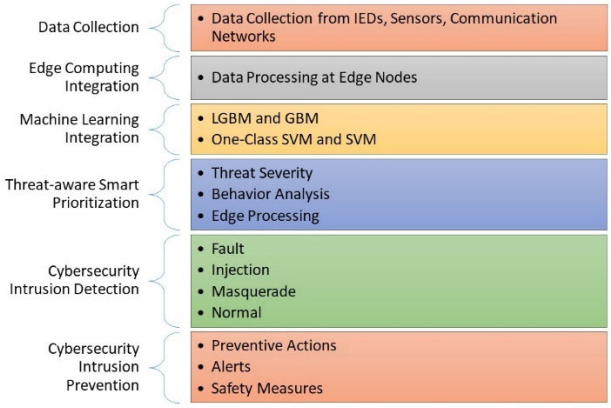


FIGURE 2. Workflow of the components of the proposed framework.

Injection attacks are a type of cybersecurity threat in which malicious data or commands are inserted into data streams in an application or system. Injection attacks on IEDs within smart grids involve the unauthorized insertion of malicious data or commands into the communication channels of the grid. Injection attacks have the ability to manipulate data transmitted between IEDs, leading to false measurements, altered sensor readings, or inaccurate status reports. This will influence decision-making processes within the smart grid. Compromising the data integrity of the smart grid data and control systems affects the trustworthiness of information and leads to cascading failures. Equation 10 mathematically represents the probability of success rate for injection attacks.

$$P\,(Injection\ success) = Vulnerability\ level \times Effectiveness\ of\ Security\ Measures \tag{10}$$

where vulnerability level reflects the existing vulnerability in smart grid IEDs and effectiveness of security measures indicates how well security measures are implemented.

In order to mitigate injection attacks, robust authentication mechanisms are required to be implemented to ensure that only authorized entities can access and control IEDs. Deployment of intrusion detection systems will provide a better solution to monitor network traffic and detect abnormal patterns indicative of injection attacks.

IV. AN EDGE COMPUTING-BASED AND THREAT BEHAVIOR-AWARE SMART PRIORITIZATION FRAMEWORK FOR CYBERSECURITY INTRUSION DETECTION IN IEDS

This study proposes a framework with the integration of edge computing, threat-aware smart prioritization, and machine learning models. The workflow of the components of the proposed framework is shown in Figure 2. The proposed

Algorithm 1 An Edge Computing-Based and Threat Behavior-Aware Smart Prioritization Framework

Input: ID (IEDs Data), SD (Sensors Data) and CND (Communication Networks Data)
Output: Prioritized Alert-based Intrusion Detection and Prevention
Procedure: Threat behavior-aware smart prioritization framework (ID, SD, CND)

1. **Parameter Initialization**
   i. α, β & γ : Weights for prioritization
   ii. $S_{threat}, S_{behavior}, S_{edge}$: Scores for severity, behavior and proceeding and edge node
   iii. Priority: Calculated priority
   iv. Alerts: List of prioritized alerts
2. **Data Collection**
   i. $Data\ Collection = (IEDs, Sensors, Communication\ Networks)$
   ii. Di : Store the collected data in a local buffer
3. **Edge Computing Processing**
   a) for each computing node i
   $Pi =$ Local_Processing (Di)
4. **Machine Learning Model Integration**
   i. Train and deploy machine learning methods
   ii. $M_{LGBM} = TrainLGBM(P_1, P_2, \ldots, P_N)$
   iii. $M_{OneClass-SVM} = TrainOneClass - SVM(P_1, P_2, \ldots, P_N)$
5. **Prioritize Alerts**
   $Priority = \left(\alpha.S_{threat} + \beta.S_{behavior} + \gamma.S_{edge}\right)$
6. **Cybersecurity Intrusion Detection**
   i. For each edge computing node i
   $A_{LGBM(i)} = ApplyLGBM(P_i, M_{LGBM})$
   $A_{OnceClass-SVM(i)} = ApplyOneClass - SVM(P_i, M_{LGBM})$
   ii. If intrusion detected on node i
   $SmartGRid\_Safety_i = Trigger\ \{PreventiveActions\ (Priority, threat\ behavior), Alert, SafetyMeasures\}$
7. **Result Generation**
   $PA - IDP = Prioritized\ Alert\ based\ Intrusion\ Detection\ and\ Prevention$
8. **Return** $\boldsymbol{PA - IDP}$

framework utilizes edge computing technology for data processing and analysis at local nodes. Modified machine learning models, i.e., LGBM and One Class-SVM have been used to detect intrusions in IEDs. A threat behavior-aware smart prioritization preventive mechanism has been defined for proactive prevention of cybersecurity intrusions in smart grid environment. Mathematically, smart prioritization is represented by equation 11.

$$Priority = \left(\alpha.S_{threat} + \beta.S_{behavior} + \gamma.S_{edge}\right) \tag{11}$$

where, α, β & γ are weighting factors, threat severity is represented by S_{threat}, behavior analysis is represented by $S_{behavior}$ and edge processing is represented by S_{edge}.

The proposed framework improves smart grid cybersecurity by integrating several components, as shown in Algorithm 1. It implements edge-computing technology for data storage and processing in smart grids, applies machine-learning models for cybersecurity intrusion detection in IEDs, and provides prevention by assigning priorities to the threats based on their behavior. In order to show the effectiveness of the proposed framework, we modified and implemented two machine-learning models, i.e., LGBM and One Class-SVM, as proposed models in the framework. For multidimensional classification and detection of cybersecurity intrusions in IEDs of smart grids, we used LGBM. Whereas, for binary classification and detection of cybersecurity intrusions, we used One Class-SVM. We simulated the detection and classification of cybersecurity intrusions in IEDs using a power system intrusion dataset. Data from sensors, communication networks, and intelligent electronic devices (IEDs) are among the inputs. Making an ordered list of alerts according to intrusion detection and severity is the main goal. The procedure starts with the initialization of parameters, with weights (α, β & γ) for scoring definition and prioritization ($S_{threat}, S_{behavior}, S_{edge}$). Information from IEDs, sensors, and communication networks are gathered for data collection, and it is then stored in a local buffer (Di). The processing of edge computing is achieved next, in which every computing node processes its local data (Pi). The framework incorporates machine learning models that have been trained on the processed data, namely LGBM and One-Class SVM. Then, with the established weights and scores, the warnings are prioritized according to a determined priority. Using the trained models, the algorithm moves on

to cybersecurity intrusion detection on every edge computing node. Safety precautions, alarms, and preventive actions are initiated for the individual node in the event that an intrusion is found. The algorithm returns the Prioritized Alert-based Intrusion Detection and Prevention (PA-IDP) result after creating the prioritized alerts based on intrusion detection and prevention.

V. EXPERIMENTS, RESULTS & DISCUSSIONS

We perform the simulations and evaluate the performance of proposed framework.

A. EVALUATION METRICS

We use the evaluation metrics of Accuracy, Precision, Recall and F1 score for evaluating the efficiency of the proposed framework [12]. These values are calculated based on the following terms True Positives (TP), True Negatives (TN), False Positives (FP) and False Negatives (FN) [15]. TP is the number of tuples that are really found to be intrusive at the end of the process. TN is the number of valid tuples that are found at the end of the detecting process. FP is the number of safe tuples that, at the conclusion of the detection process, are identified as intrusions. FN is the quantity of dangerous tuples that, at the conclusion of the detection process, are found normally.

Accuracy is an employed metric for evaluating the performance of classification models [15]. Mathematically, it is calculated with the help of Equation 12.

$$A = \frac{TP + TN}{TP + TN + FP + FN} \tag{12}$$

Precision is a metric used to assess the efficacy of a classification model [15]. Mathematically, it is represented by Equation 13.

$$Precision = \frac{TP}{TP + FP} \tag{13}$$

Recall is a metric used to assess a classification model's performance [15]. Mathematically, it is given by Equation 14.

$$Recall = \frac{TP}{TP + FN} \tag{14}$$

The F1 score is a way to measure how well classification models work, especially when they are asked to choose between two options [15]. Mathematically, it is calculated with the help of Equation 15.

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{15}$$

B. DATASET

In order to evaluate the proposed framework, ''Power System Intrusion Dataset'' [43], a publicly available dataset on a Kaggle website has been used. Digital electrical substations form the backbone of Smart Grids, and the implementation of IEC-61850 standards for communication among IEDs introduces new security challenges. Ensuring the proper operation of digital substation services requires effective intrusion detection and prevention mechanisms, which were previously lacking for attacks such as masquerade and replay in smart grid environments. The dataset includes data on faults, injections, replay, and masquerade attacks. The distribution of components in the dataset is illustrated in Figure 3. Key variables in the dataset are as follows:

- sqNum and stnum are IDs or counters representing sequence or status numbers.
- state_cb indicates the binary state.
- Differences in status or sequence numbers (sqDiff, stDiff) indicate changes over time.
- timeLastMsg provides the duration since the last event or message.
- recentChange is a binary indicator of a recent occurrence or change.
- MU1Cs, MU2Cs, etc., are measurements from multiple units (MU).
- MU4VoltageAngleA, MU4VoltageAngleB, and MU4VoltageAngleC represent voltage angles in a three-phase system.
- Additional readings, such as current measurements for CMU4, IED4_iA, IED4_iB, and IED4_iC, are included.
- MU4Log indicates the engagement of a relay or similar component.

The class variable, indicating system status, includes categories such as 'Normal', 'Fault', 'Injection', 'Masquerade', and 'Replay'. 'Normal' is the most prevalent class. The variable distribution, as shown in Figure 4, highlights the class disparity used for modeling. The dataset size is relatively small; however, it contains sufficient instances that are highly relevant to our study and meet the requirements of our proposed framework. The main limitation of the dataset is its specific focus on IEDs, which aligns with the targeted scope of our study on IEDs in smart grids. In the future, our aim is not only to expand the dataset with additional relevant entries but also to integrate it with other smart grid datasets.

C. EXPERIMENTAL DESIGN

A power system intrusion dataset has been used for evaluation, and it is divided into two parts: the training set and the test set. The training set comprised 80% of the total records in the dataset. It was used to train the proposed models. On the other hand, the test set comprised 20% of the total number of records. It was used to test and validate the proposed model. Cross-validation was also performed for LGBM through the ''cross_val_score'' function from scikit-learn. However, for One Class-SVM, we validated the model using a train-test split with an 80:20 ratio since cross-validation is not applicable due to its unsupervised learning nature. We implemented all experiments in Python on a GPU-based system with a 1.8 GHz CPU and 12 GB of RAM. Predefined machine learning packages and libraries, namely Pandas, Numpy, Seaborn, Sklearn and Matplotlib, have been used.

D. RESULTS AND EVALUATION

We modified and implemented two machine-learning models, i.e., LGBM and One Class-SVM, as proposed models

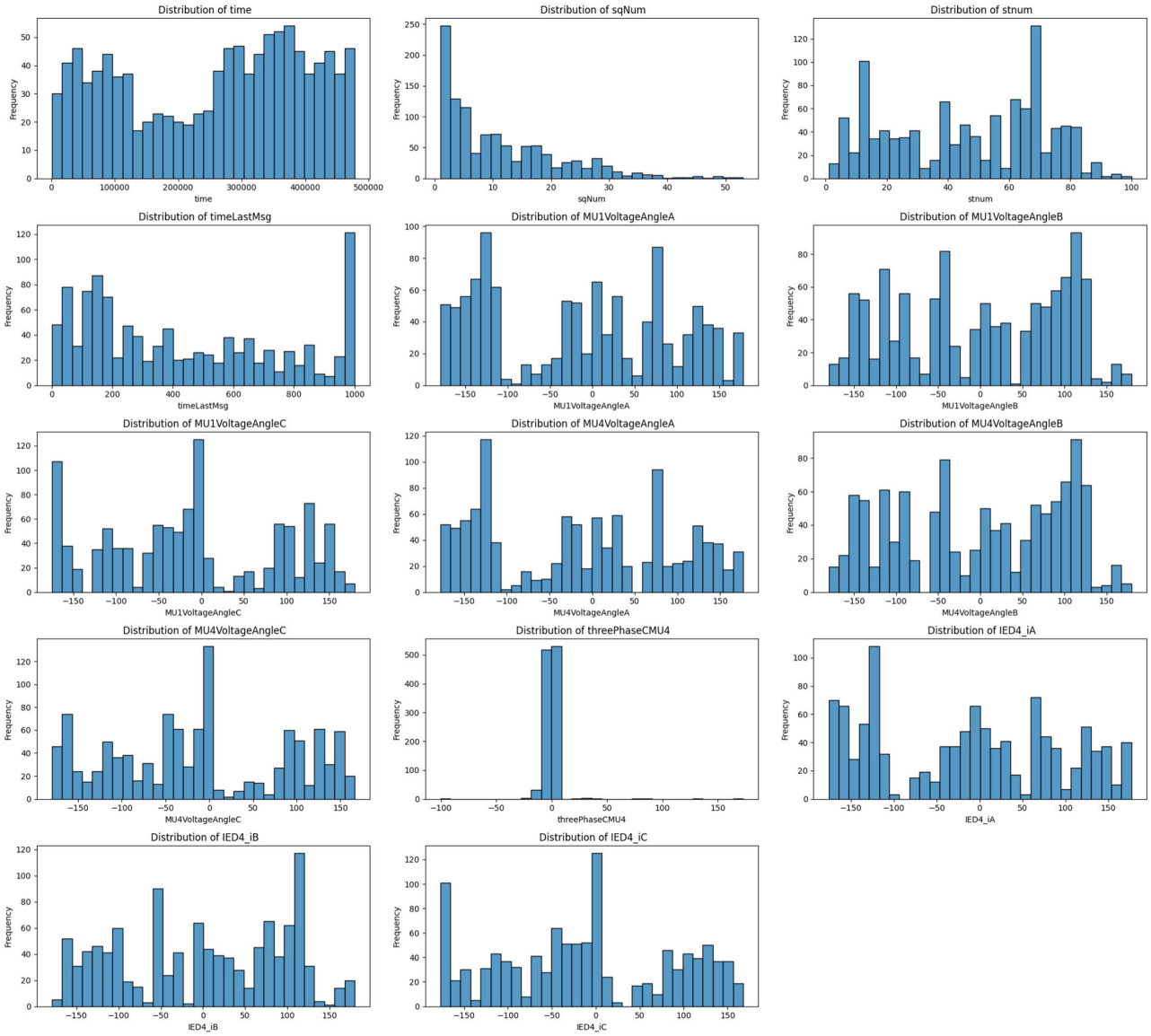


FIGURE 3. Distribution of components in a dataset.

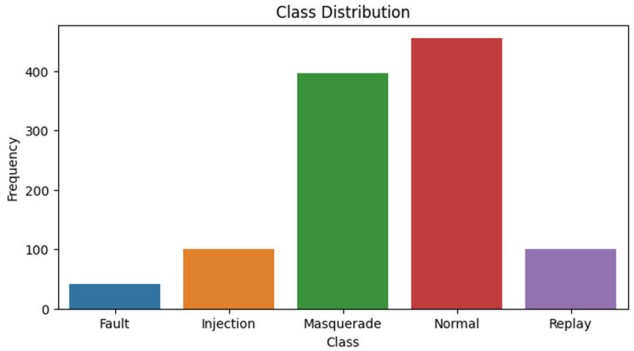


FIGURE 4. Class variable distribution.

in the framework. For multidimensional classification and detection of cybersecurity intrusions in IEDs of smart grids, we used LGBM. LGBM is suitable for real-time data analysis due to its efficiency and speed with constrained resources. In edge computing environments, LGBM has the ability to handle large datasets quickly with constrained computing resources as compared with cloud computing. LGBM employs a parallel learning technique, and it is best suited for distributed computing environments to execute a large number of tasks concurrently. LGBM has the ability to handle imbalanced datasets for accurate analysis, and intrusion detection datasets often exhibit imbalanced class distributions. For binary classification and detection of cybersecurity intrusions, we used One Class-SVM. As reflected in the name, One Class-SVM has the ability to train only on a single class, i.e., normal instances and then it identifies deviations from normal behavior as anomalies. In smart grids, the majority of the data represents normal operations; therefore,

TABLE 1. Classification report generated by LGBM and GBM.

Classification	Precession		Recall		F1-Score		Support	Accuracy	
	LGBM	GBM	LGBM	GBM	LGBM	GBM		LGBM	GBM
Fault	0.89	0.89	1.00	1.00	0.94	0.94	8	0.93	0.90
Injection	1.00	0.81	0.56	0.68	0.72	0.74	25		
Masquerade	0.96	0.96	0.99	0.94	0.98	0.95	82		
Normal	0.92	0.91	0.97	0.98	0.94	0.94	88		
Replay	0.80	0.71	1.00	0.62	0.89	0.67	16		
Macro Average	0.92	0.86	0.90	0.84	0.89	0.85	219		
Weighted Average	0.94	0.90	0.93	0.90	0.93	0.90	219		

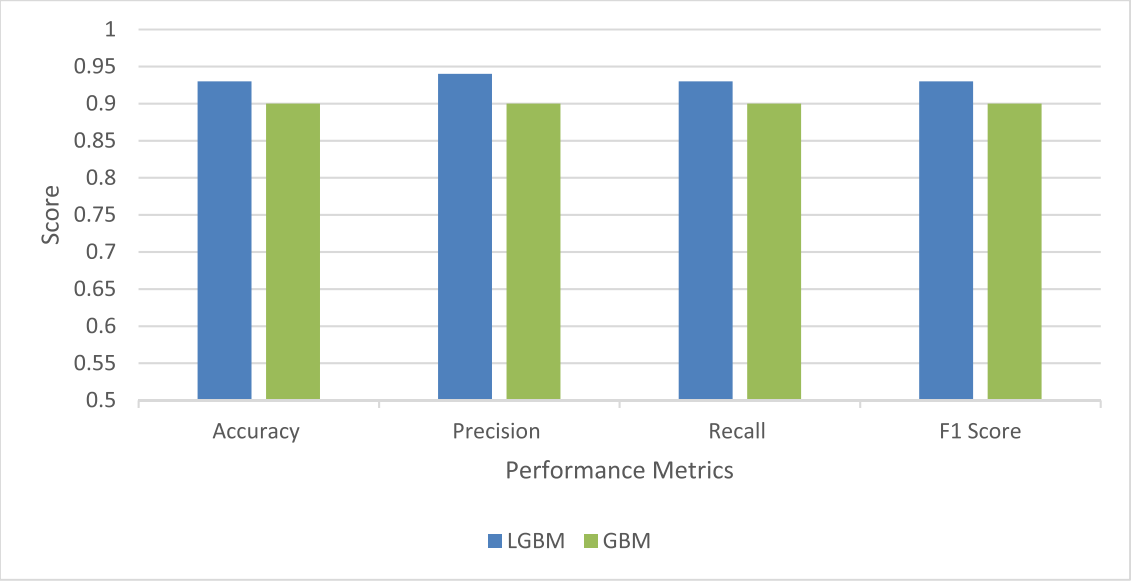


FIGURE 5. LGBM and GBM performance metrics.

this approach is best suited for the detection of intrusions. Intrusion detection datasets often exhibit imbalanced class distributions, and thus, in such situations, One Class-SVM is best suited as it focuses on modeling the normal class while identifying deviations.

We made modifications to LGBM to enhance its performance in addressing the specific problem of intrusion detection in IEDs of smart grids. We enhanced the sensed feature of LGBM in its data inputs with unusual network activities and unexpected access patterns. We performed multidimensional detection and classification, including masquerade attacks, replay attacks, injections and normal instances. We also incorporated the features of IED behavior and communication patterns, performed hyperparameter tuning and selected parameters specific to intrusion detection in IEDs. On the other hand, we modified and implemented One Class-SVM for binary classification since it has the ability to recognize normal instances in the dataset. However, not all the other activities or instances in the dataset are intrusions. Therefore, in order to enhance accuracy and perform better analysis, we redefined the normal instances and anomalies in the power system intrusion dataset. We also tailor the sensitivity of One Class-SVM by modifying the fine-tuning parameter value 'nu' to precisely identify deviations that are significantly potential security breaches for IEDs in smart grids.

We implemented the benchmark machine-learning models, i.e., Gradient Boosting Machine (GBM) [44], [45] and Support Vector Machine (SVM) [46], [47], for performance comparison with the proposed modified machine-learning models. The evaluation results are highlighted below:

1) LGBM AND GRADIENT BOOSTING

Light Gradient Boosting Machine (LGBM) is a powerful machine learning algorithm that has the ability to been used in a number of domains, including smart grid systems for intrusion detection [35]. LGBM is a member of the gradient boosting framework within the ensemble learning family. It is renowned for its effectiveness, speed, and capacity to manage huge, highly dimensional datasets. As LGBM can effectively manage massive amounts of data produced by sensors, communication networks, and Intelligent Electronic Devices (IEDs), therefore, it is best suitable for intrusion detection in smart grids. Numerous data points are present in the smart grid environment, and LGBM speedy data processing makes

TABLE 2. Classification report generated by One Class-SVM and SVM.

Classification	Precession		Recall		F1-Score		Support	Accuracy	
	OC-SVM	SVM	OC-SVM	SVM	OC-SVM	SVM		OC-SVM	SVM
Anomaly	0.96	0.80	0.86	0.81	0.91	0.80	639	0.85	0.77
Normal	0.44	0.73	0.74	0.71	0.55	0.72	91		
Macro Average	0.70	0.76	0.80	0.76	0.73	0.76	730		
Weighted Average	0.89	0.77	0.85	0.77	0.86	0.77	730		

it useful for real-time threat detection. The gradient boosting framework used by LGBM is especially useful for enhancing intrusion detection model accuracy. The program creates a chain of inexperienced learners, fixing each other's mistakes as it goes. The model overall forecast accuracy is improved by this sequential learning technique, which is important for spotting emerging and subtle cyber threats in smart grid systems. When it comes to smart grid security, datasets is unbalanced, with most cases showing typical system behavior and very few potentially intrusive instances. As LGBM is adept at handling unbalanced datasets, it can detect infrequent occurrences of cyber threats without favoring the dominant class. Edge computing is frequently used in smart grid applications to process data locally. As LGBM is able to be installed on edge devices and is adaptable to this computing paradigm, it identify intrusions more quickly and locally without depending entirely on centralized processing.

Table 1 shows the classification report generated by LGBM, GBM and it is further visualized by Figure 5. High efficacy is shown by the outcomes of using the LGBM for intrusion detection in a smart grid infrastructure. The precision values show how well the model classified instances of each sort of intrusion. The high level of precision attained for the 'Injection' class, which suggests a low false positive rate. The model, however, overlook certain occurrences of this kind of intrusion, as indicated by the low recall for "Injection." The 'Masquerade' class demonstrates outstanding recall and precision, indicating that the model can correctly detect and distinguish between masquerade attack cases. The ability of model to accurately classify occurrences across all sorts of intrusions is demonstrated by its overall accuracy of 93%. The performance is consistently resilient, as evidenced by F1-scores above 0.89 for both the weighted average (which takes into account class imbalance) and the macro-average (which gives equal weight to each class). This shows that the LGBM model is capable of dependable intrusion detection in the intricate and dynamic smart grid environment by effectively striking a compromise between decreasing false positives and false negatives. The findings suggest that the LGBM model is a useful tool for preserving the integrity and dependability of vital infrastructure since it is well suited for protecting smart grid systems against a range of intrusion scenarios.

The confusion matrix produced by the LGBM model is shown in Figure 6 that provides a summary of its performance

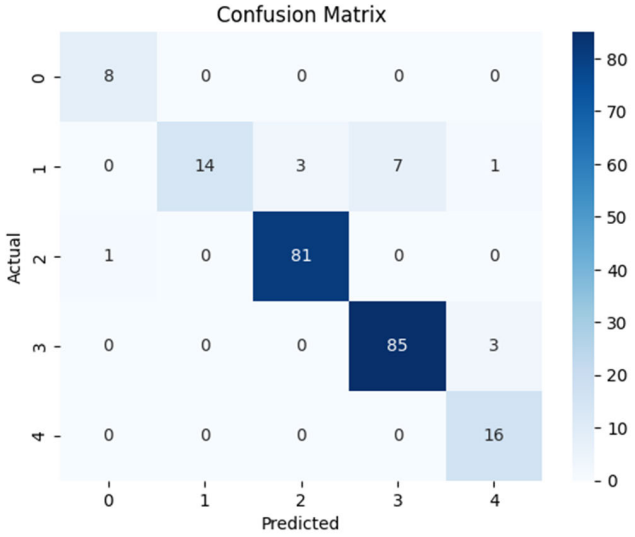


FIGURE 6. LGBM confusion matrix.

across several classes—Fault, Injection, Masquerade, Normal, and Replay. A diagonal entry of eight in the first row indicates that the model properly recognized every occurrence of the 'Fault' class. This shows that there are neither false positives nor false negatives for the Fault class, indicating flawless precision and recall. While the 'Injection' class shows a respectable 14 true positives, the existence of 3 false positives and 7 false negatives points to potential problems. While the model accurately detects injections, it also misclassifies certain injections and ignores others. As indicated by the high true positives (81) the model does remarkably well in identifying instances of "Masquerade". For this class, there are neither false positives nor false negatives, showing almost flawless precision and recall. The 'Normal' class performs admirably as well, yielding a high percentage of true positives (85). Notwithstanding, the existence of false negatives (3) implies that the model might overlook a small number of 'Normal' activity occurrences. The 'Replay' class, like the 'Fault' and 'Masquerade' classes, achieves flawless recall and precision with 16 true positives and 0 false negatives or false positives.

2) ONE CLASS-SVM AND SVM

One-Class Support Vector Machine (One-Class SVM) is a machine learning model used for anomaly identification in

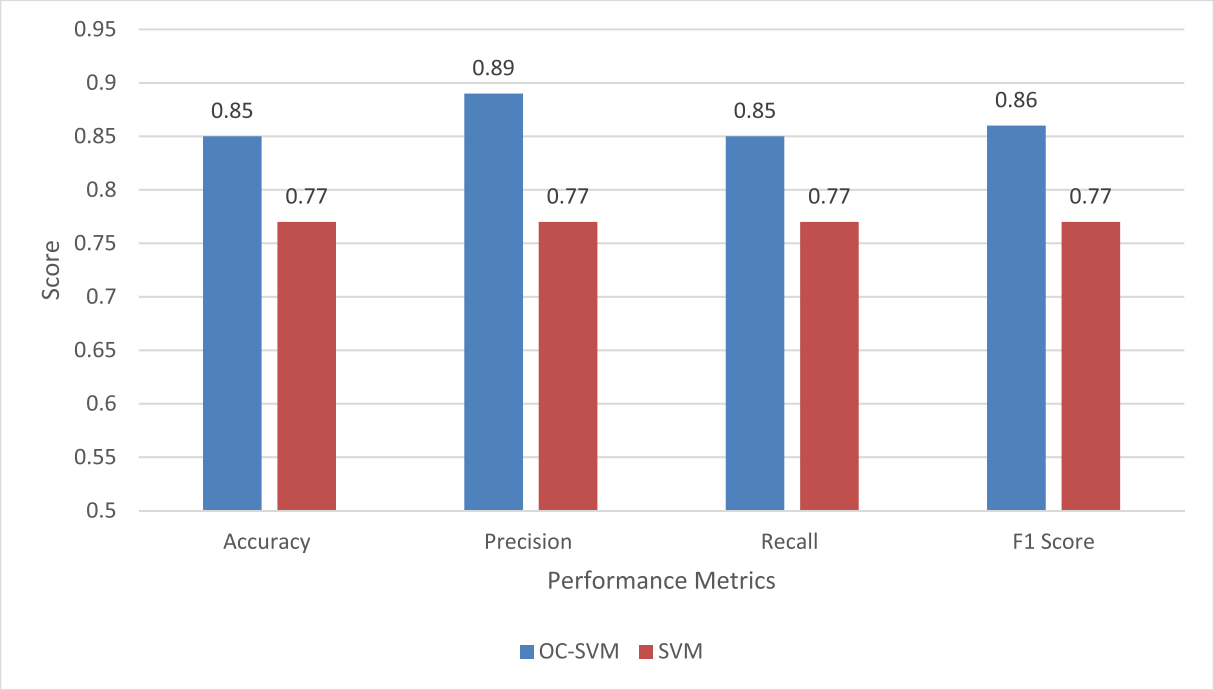


FIGURE 7. One Class-SVM and SVM performance metrics.

datasets where one class is a major or normal class [12], [36]. The One-Class SVM is quite useful in detecting odd or aberrant behavior that deviates from the norm and an indication of an intrusion or a security risk when it comes to intrusion detection within a smart grid system. One-Class SVM is intended to identify and learn a boundary or hyperplane surrounding the normal data instances. By treating them as exemplars of typical behavior within the smart grid system, it seeks to summarize most of the data points. One-Class SVM is used in an unsupervised learning environment, in contrast to regular SVMs. Labeled data containing examples of both normal and intrusive conduct are not necessary. Rather, it concentrates on learning the regular data patterns during training, which makes it appropriate for situations in which labeled incursion events may be hard to come by or unavailable. The One-Class SVM frequently makes use of the kernel trick to convert the data into a higher-dimensional space, which enables it to more successfully identify a hyperplane that divides the typical cases from any possible outliers or incursions. One-Class SVMs are good at spotting deviations or outliers and have an impact on the detection accuracy and boundary definition. The One-Class SVM is useful for intrusion detection in a smart grid infrastructure by identifying patterns of typical grid activity from data gathered from a variety of components, including sensors, communication networks, and IEDs.

Table 2 shows the classification report generated by One Class-SVM, SVM and it is further visualized by Figure 7. The classification report shows the findings of One-Class SVM findings for intrusion detection in the smart grid environment. With a comparatively low false positive rate, the precision of 0.96 for anomalies indicates a good accuracy in accurately recognizing instances tagged as anomalies. Recall of 0.86, on the other hand, suggests that the model have overlooked some real abnormalities, highlighting the need to balance recall and precision. Conversely, the recall of 0.74 indicates that a considerable proportion of true normal examples were accurately identified, although the precision of 0.44 for normal instances points to a high false positive rate. The percentage of accurately identified instances is reflected in the total accuracy of 0.85. The weighted average F1-score of 0.86 and the macro average of 0.73, respectively, offer a balanced assessment of recall and precision for both groups. There is potential for improvement in recall for both the anomaly and normal classes, even though the model shows good precision for anomalies, showing confidence in the recognized occurrences.

Figure 8 shows One Class-SVM confusion matrix, in which 552 occurrences were accurately classified as anomalies (True Positives) by the model. This shows the times when the unusual activity in the smart grid was correctly identified and categorized by the model. There were 87 cases when normal behavior was seen in places where anomalies were predicted. This implies situations when regular actions were wrongly categorized as abnormal by the model. There are 24 real abnormalities which were missed by the model, which consequently classified them as False Negatives. There are 67 occurrences which were accurately classified as normal behavior by the model (True Negatives). The high percentage of true positives demonstrates

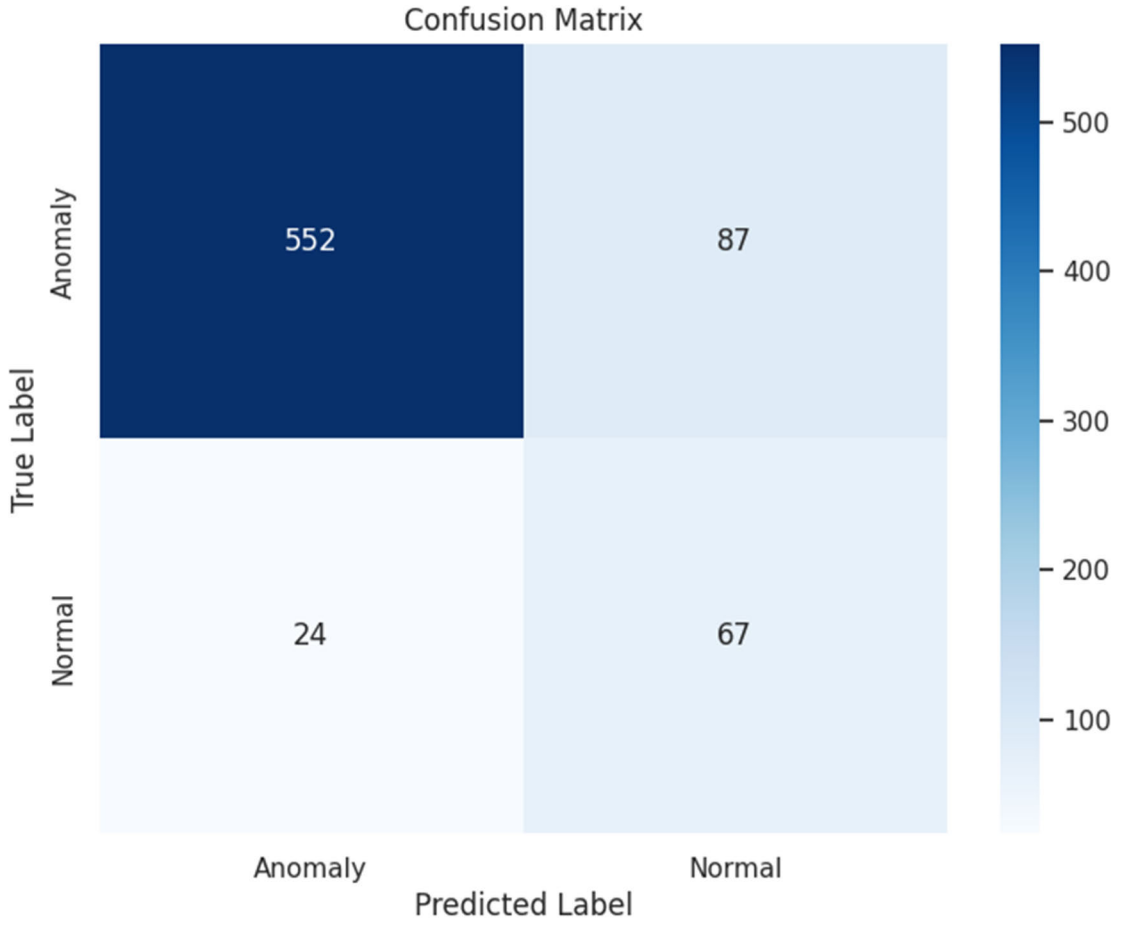


FIGURE 8. One Class-SVM confusion matrix.

the model great capacity to detect anomalies accurately, which is consistent with the categorization of high accuracy for anomalies. A possible area for improvement is highlighted by the false positives, where a significant number of regular cases were wrongly identified as anomalies by the model. This implies that adjustments are necessary to improve specificity and decrease false positives. The true negatives represent the cases in which the model accurately detected typical behavior.

VI. CONCLUSION AND FUTURE WORK

For cybersecurity intrusion detection and prevention in smart grid environments, we proposed edge computing-based and threat behavior-aware smart prioritization framework. The proposed framework uses modified LGBM and One Class-SVM methods. The proposed framework represents a major advancement in bolstering the dependability and resilience of contemporary electrical infrastructures. The study presents a comprehensive strategy that combines edge-computing, machine learning algorithms, and behavior-aware methodologies, with a particular emphasis on resolving the cybersecurity issues related to IEDs in smart grids. The main goal of the study was to improve smart grid cybersecurity protocols as smart grids are becoming more and more integrated into energy distribution networks, which has led to an increase in cybersecurity risks. The proposed framework progresses the creation of cybersecurity procedures made especially for smart grid settings. The system offers an improved defense mechanism against intrusion attempts on IEDs by combining behavior-aware techniques with modified machine learning algorithms. A smart prioritizing mechanism has been adopted in the framework that rates the urgency and seriousness of detected incursions. This makes it possible to allocate resources more wisely and respond to serious security problems quickly. The priority method takes into account the impact on the smart grid functionality as well as the criticality of the affected devices. We simulated the detection and classification of cybersecurity intrusions in IEDs using a power system intrusion dataset. The LGBM model accurately finds and classifies cybersecurity breaches in IEDs of smart grids, achieving an accuracy of 93%, a precision of 94%, a recall of 93%, and an F1 score of 93%. The implementation of One Class-SVM with binary classification yields an accuracy of 85%, precision of 89%, recall of 85%, and F1

score of 86%. The models demonstrate equilibrium in both precision and recall metrics, highlighting their dependability in intrusion detection situations.

In the future, this work will be extended by the integration of energy-efficient techniques for smart grid environments. A machine-learning-based incident response and recovery system will also be implemented in a smart grid environment. Hybrid approaches will also be utilized for the detection and classification of cybersecurity intrusions in the communication networks of smart grids.

ACKNOWLEDGMENT

The authors sincerely appreciate the support from the Deanship of Scientific Research at King Khalid University under research grant number (R.G.P.2/93/45).

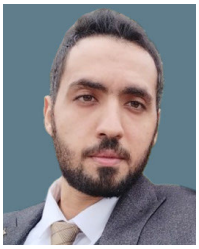
REFERENCES

[1] G. Dileep, "A survey on smart grid technologies and applications," *Renew. Energy*, vol. 146, pp. 2589–2625, Feb. 2020, doi: 10.1016/j.renene.2019.08.092.
[2] B. S. Torres, L. E. Borges da Silva, C. P. Salomon, and C. H. V. de Moraes, "Integrating smart grid devices into the traditional protection of distribution networks," *Energies*, vol. 15, no. 7, p. 2518, Mar. 2022, doi: 10.3390/en15072518.
[3] F. E. Abrahamsen, Y. Ai, and M. Cheffena, "Communication technologies for smart grid: A comprehensive survey," *Sensors*, vol. 21, no. 23, p. 8087, Dec. 2021, doi: 10.3390/s21238087.
[4] V. Kulkarni, S. K. Sahoo, S. B. Thanikanti, S. Velpula, and D. I. Rathod, "Power systems automation, communication, and information technologies for smart grid: A technical aspects review," *TELKOMNIKA (Telecommunication Comput. Electron. Control)*, vol. 19, no. 3, p. 1017, Jun. 2021, doi: 10.12928/telkomnika.v19i3.16428.
[5] S. K. Rathor and D. Saxena, "Energy management system for smart grid: An overview and key issues," *Int. J. Energy Res.*, vol. 44, no. 6, pp. 4067–4109, May 2020, doi: 10.1002/er.4883.
[6] A. Algarni, I. Shah, A. I. Jehangiri, M. A. Ala'Anzy, and Z. Ahmad, "Predictive energy management for Docker containers in cloud computing: A time series analysis approach," *IEEE Access*, vol. 12, pp. 52524–52538, 2024, doi: 10.1109/ACCESS.2024.3387436.
[7] F. Bonavolontà, V. Caragallo, A. Fatica, A. Liccardo, A. Masone, and C. Sterle, "Optimization of IEDs position in MV smart grids through integer linear programming," *Energies*, vol. 14, no. 11, p. 3346, Jun. 2021, doi: 10.3390/en14113346.
[8] M. Alonso, H. Amaris, D. Alcala, and D. M. Florez, "Smart sensors for smart grid reliability," *Sensors*, vol. 20, no. 8, p. 2187, Apr. 2020, doi: 10.3390/s20082187.
[9] M. Orlando, A. Estebsari, E. Pons, M. Pau, S. Quer, M. Poncino, L. Bottaccioli, and E. Patti, "A smart meter infrastructure for smart grid IoT applications," *IEEE Internet Things J.*, vol. 9, no. 14, pp. 12529–12541, Jul. 2022, doi: 10.1109/JIOT.2021.3137596.
[10] M. Rashed, I. Gondal, J. Kamruzzaman, and S. Islam, "State estimation within IED based smart grid using Kalman estimates," *Electronics*, vol. 10, no. 15, p. 1783, Jul. 2021, doi: 10.3390/electronics10151783.
[11] S. R. Biswal, T. Roy Choudhury, B. Panda, B. Nayak, and G. C. Mahato, "Smart meter: Impact and usefulness on smart grids," in *Proc. IEEE 2nd Int. Conf. Appl. Electromagn., Signal Process., Commun. (AESPC)*, Nov. 2021, pp. 1–6, doi: 10.1109/AESPC52704.2021.9708492.
[12] W. M. S. Yafooz, Z. B. A. Bakar, S. K. A. Fahad, and A. M. Mithon, "Business intelligence through big data analytics, data mining and machine learning," in *Proc. Data Manag., Anal. Innov.*, vol. 1016, 2020, pp. 217–230, doi: 10.1007/978-981-13-9364-8_17.
[13] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey," *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–20, Dec. 2018, doi: 10.1186/s13677-018-0123-6.
[14] F. Al-Quayed, Z. Ahmad, and M. Humayun, "A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0," *IEEE Access*, vol. 12, pp. 34800–34819, 2024, doi: 10.1109/ACCESS.2024.3372187.
[15] A. Kumari, R. K. Patel, U. C. Sukharamwala, S. Tanwar, M. S. Raboaca, A. Saad, and A. Tolba, "AI-empowered attack detection and prevention scheme for smart grid system," *Mathematics*, vol. 10, no. 16, p. 2852, Aug. 2022, doi: 10.3390/math10162852.
[16] S. Kumar and R. R. Mallipeddi, "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions," *Prod. Operations Manage.*, vol. 31, no. 12, pp. 4488–4500, Dec. 2022, doi: 10.1111/poms.13859.
[17] A. Corallo, M. Lazoi, M. Lezzi, and P. Pontrandolfo, "Cybersecurity challenges for manufacturing systems 4.0: Assessment of the business impact level," *IEEE Trans. Eng. Manag.*, vol. 70, no. 11, pp. 3745–3765, Nov. 2023, doi: 10.1109/TEM.2021.3084687.
[18] A. Corallo, M. Lazoi, and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Comput. Ind.*, vol. 114, Jan. 2020, Art. no. 103165, doi: 10.1016/j.compind.2019.103165.
[19] V. Mullet, P. Sondi, and E. Ramat, "A review of cybersecurity guidelines for manufacturing factories in industry 4.0," *IEEE Access*, vol. 9, pp. 23235–23263, 2021, doi: 10.1109/ACCESS.2021.3056650.
[20] T. M. Fernández-Caramés and P. Fraga-Lamas, "Use case based blended teaching of IIoT cybersecurity in the industry 4.0 era," *Appl. Sci.*, vol. 10, no. 16, p. 5607, Aug. 2020, doi: 10.3390/app10165607.
[21] L. F. Ilca, O. P. Lucian, and T. C. Balan, "Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response," *Sensors*, vol. 23, no. 15, p. 6757, Jul. 2023, doi: 10.3390/s23156757.
[22] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0305–0310, doi: 10.1109/CCWC.2019.8666450.
[23] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.
[24] A. U. Rehman, Z. Ahmad, A. I. Jehangiri, M. A. Ala'Anzy, M. Othman, A. I. Umar, and J. Ahmad, "Dynamic energy efficient resource allocation strategy for load balancing in fog environment," *IEEE Access*, vol. 8, pp. 199829–199839, 2020, doi: 10.1109/ACCESS.2020.3035181.
[25] M. Ali, A. I. Jehangiri, O. I. Alramli, Z. Ahmad, R. M. Ghoniem, M. A. Ala'anzy, and R. Saleem, "Performance and scalability analysis of SDN-based large-scale Wi-Fi networks," *Appl. Sci.*, vol. 13, no. 7, p. 4170, Mar. 2023, doi: 10.3390/app13074170.
[26] W. Saeed, Z. Ahmad, A. I. Jehangiri, N. Mohamed, and A. I. Umar, "A fault tolerant data management scheme for healthcare Internet of Things in fog computing," *KSII Trans. Internet Inf. Syst.*, vol. 15, no. 1, pp. 35–57, 2021.
[27] A. Algarni, T. Acarer, and Z. Ahmad, "An edge computing-based preventive framework with machine learning-integration for anomaly detection and risk management in maritime wireless communications," *IEEE Access*, vol. 12, pp. 53646–53663, 2024, doi: 10.1109/ACCESS.2024.3387529.
[28] C. Gomez, S. Chessa, A. Fleury, G. Roussos, and D. Preuveneers, "Internet of Things for enabling smart environments: A technology-centric perspective," *J. Ambient Intell. Smart Environments*, vol. 11, no. 1, pp. 23–43, Jan. 2019, doi: 10.3233/ais-180509.
[29] M. Diyan, B. Nathali Silva, J. Han, Z. Cao, and K. Han, "Intelligent Internet of Things gateway supporting heterogeneous energy data management and processing," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 2, pp. 1–15, Feb. 2022, doi: 10.1002/ett.3919.
[30] R. M. Abdelmoneem, A. Benslimane, and E. Shaaban, "Mobility-aware task scheduling in cloud-fog IoT-based healthcare architectures," *Comput. Netw.*, vol. 179, Oct. 2020, Art. no. 107348, doi: 10.1016/j.comnet.2020.107348.
[31] P. R. R. De Souza, K. J. Matteussi, A. D. S. Veith, B. F. Zanchetta, V. R. Q. Leithardt, Á. L. Murciego, E. P. De Freitas, J. C. S. D. Anjos, and C. F. R. Geyer, "Boosting big data streaming applications in clouds with BurstFlow," *IEEE Access*, vol. 8, pp. 219124–219136, 2020, doi: 10.1109/ACCESS.2020.3042739.
[32] Z. H. Kok, A. R. Mohamed Shariff, M. S. M. Alfatni, and S. Khairunniza-Bejo, "Support vector machine in precision agriculture: A review," *Comput. Electron. Agricult.*, vol. 191, Dec. 2021, Art. no. 106546, doi: 10.1016/j.compag.2021.106546.
[33] W. Modesto, L. Bastos, A. V. Neto, D. Rosário, and E. Cerqueira, "Towards automating the integration of legacy IEDs into edge-supported Internet of Smart grid things," *J. Internet Services Appl.*, vol. 13, no. 1, pp. 33–45, Nov. 2022, doi: 10.5753/jisa.2022.2374.

[34] U. AlHaddad, A. Basuhail, M. Khemakhem, F. E. Eassa, and K. Jambi, "Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks," *Sensors*, vol. 23, no. 17, p. 7464, Aug. 2023, doi: 10.3390/s23177464.
[35] O. D. Okey, S. S. Maidin, P. Adasme, R. L. Rosa, M. Saadi, D. C. Melgarejo, and D. Z. Rodríguez, "BoostedEnML: Efficient technique for detecting cyberattacks in IoT systems using boosted ensemble machine learning," *Sensors*, vol. 22, no. 19, p. 7409, Sep. 2022, doi: 10.3390/s22197409.
[36] A. Binbusayyis and T. Vaiyapuri, "Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and one-class SVM," *Appl. Intell.*, vol. 51, no. 10, pp. 7094–7108, Oct. 2021, doi: 10.1007/s10489-021-02205-9.
[37] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An effective intrusion detection approach based on ensemble learning for IIoT edge computing," *J. Comput. Virol. Hacking Techn.*, vol. 19, no. 4, pp. 469–481, Dec. 2022, doi: 10.1007/s11416-022-00456-9.
[38] S. E. Quincozes, C. Albuquerque, D. Passos, and D. Mossé, "A survey on intrusion detection and prevention systems in digital substations," *Comput. Netw.*, vol. 184, Jan. 2021, Art. no. 107679, doi: 10.1016/j.comnet.2020.107679.
[39] F. Harrou, B. Bouyeddou, A. Dairi, and Y. Sun, "Exploiting autoencoder-based anomaly detection to enhance cybersecurity in power grids," *Future Internet*, vol. 16, no. 6, p. 184, May 2024, doi: 10.3390/fi16060184.
[40] A. Presekal, A. Ştefanov, V. S. Rajkumar, and P. Palensky, "Cyber forensic analysis for operational technology using graph-based deep learning," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2023, pp. 1–7, doi: 10.1109/smartgridcomm57358.2023.10333922.
[41] D. Jay, "Deception technology based intrusion protection and detection mechanism for digital substations: A game theoretical approach," *IEEE Access*, vol. 11, pp. 53301–53314, 2023, doi: 10.1109/ACCESS.2023.3279504.
[42] S. Kumar, A. Abu-Siada, N. Das, and S. Islam, "Review of the legacy and future of IEC 61850 protocols encompassing substation automation system," *Electronics*, vol. 12, no. 15, p. 3345, Aug. 2023, doi: 10.3390/electronics12153345.
[43] Kaggle. *Power System Intrusion Dataset*. Accessed: Dec. 20, 2023. [Online]. Available: https://www.kaggle.com/datasets/sequincozes/power-system-intrusion-dataset
[44] C. Bentéjac, A. Csörgő, and G. Martínez-Muñoz, "A comparative analysis of gradient boosting algorithms," *Artif. Intell. Rev.*, vol. 54, no. 3, pp. 1937–1967, Mar. 2021, doi: 10.1007/s10462-020-09896-5.
[45] A. V. Konstantinov and L. V. Utkin, "Interpretable machine learning with an ensemble of gradient boosting machines," *Knowledge-Based Syst.*, vol. 222, Jun. 2021, Art. no. 106993, doi: 10.1016/j.knosys.2021.106993.
[46] S. Suthaharan, "Support vector machine," in *Machine Learning Models and Algorithms for Big Data Classification* (Integrated Series in Information Systems), vol. 36. Boston, MA, USA: Springer, 2016, doi: 10.1007/978-1-4899-7641-3_9.
[47] J. Cervantes, F. Garcia-Lamont, L. Rodríguez-Mazahua, and A. Lopez, "A comprehensive survey on support vector machine classification: Applications, challenges and trends," *Neurocomputing*, vol. 408, pp. 189–215, Sep. 2020, doi: 10.1016/j.neucom.2019.10.118.

ABDULMOHSEN ALGARNI received the Ph.D. degree from the Queensland University of Technology, Australia, in 2012. He was a Research Associate with the School of Electrical Engineering and Computer Science, Queensland University of Technology, in 2012. He is currently an Associate Professor with the College of Computer Science, King Khalid University. His research interests include artificial intelligence, data mining, text mining, machine learning, information retrieval, and information filtering.

ZULFIQAR AHMAD received the M.Sc. degree (Hons.) in computer science from Hazara University, Mansehra, Pakistan, in 2012, the M.S. degree in computer science from COMSATS University Islamabad, Abbottabad, Pakistan, in 2016, and the Ph.D. degree in computer science from the Department of Computer Science and Information Technology, Hazara University, in 2022. He is currently serving as a Lecturer with the Department of CS and IT at Hazara University. He is the author of several publications in the fields of fog computing, cloud computing, high-performance computing, and scientific workflow execution and management. His research interests include scientific workflow management in cloud computing, the Internet of Things, fog computing, edge computing, cybersecurity, and wireless sensor networks (WSNs).



MOHAMMED ALAA ALA'ANZY received the Ph.D. degree in computer science from University Putra Malaysia (UPM), in 2023.

He is currently an Assistant Professor with Suleyman Demirel University (SDU). He specializes in cutting-edge fields, such as algorithms, cloud computing, green computing, load balancing, task scheduling, and fog computing. He is widely recognized for his substantial contributions to the academic community through high-impact journals and conference publications. In addition, he plays a pivotal role as a respected reviewer for esteemed journals, such as IEEE, Elsevier, and Springer.