SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I2P114

Volume 12 Issue 2, 152-165, February 2025
© 2025 Seventh Sense Research Group®

Original Article

Multistage Intrusion Detection Framework Using a Robust Nonlinear Machine Learning Approach for Enhancing Cloud Security in Electric Vehicles in Smart Grid

S. Selvakumari[1], K. Prabhakar[2], S. Selvakumaran[3], Mythili Nagalingam[4], C. Tamilselvi[5], T.A. Mohanaprakash[6]

[1]*Department of Physics, Panimalar Engineering College, Chennai, Tamilnadu, India.*
[2] *Department of CSE(AIML), School of Engineering and Technology, CMR University, Bangalore, Karnataka, India.*
[3]*Department of AI and DS, Rajalakshmi Institute of Technology, Chennai, Tamilnadu, India.*
[4]*Department of Computer Science and Engineering, St. Joseph's Institute of Technology, OMR, Chennai, Tamilnadu, India.*
[2]*Department of IT, Dr. MGR Educational and Research Institute Chennai, Tamilnadu, India.*
[6]*Department of IT, SOET, CMR University, Bengaluru, Karnataka, India.*

[6]*Corresponding Author : tamohanaprakash@gmail.com*

Received: 05 November 2024 Revised: 11 December 2024 Accepted: 02 January 2025 Published: 30 January 2025

Abstract *- Ensuring resilient and reliable operations requires addressing new Cloud security risks brought out by the integration of Electric Vehicles (EVs) into the ever-changing smart grids. Regarding energy distribution, vehicle operations, and public safety, the importance of a secure infrastructure in this context is essential, a single attack might cause major disruptions. However, designing effective Intrusion Detection Systems (IDS) is made more difficult by the dynamic and distributed nature of smart grids and the increasing complexity of cyberattacks. Within smart grids and smart cities, there is a multi-stage system called the Multitiered Intrusion Detection Framework utilising the Machine Learning Approach (MIDF-MLA) that aims to detect and mitigate attacks targeting EVs. To overcome these challenges, this paper proposes the MIF-MLA, using a strong, nonlinear machine learning model that can adapt to new threats by improving detection accuracy and decreasing false positives. The multi-stage architecture of MIDF-MLA is designed to address a wide range of attack vectors, including not limited to Distributed Denial-of-Service (DDoS) attacks, spoofing, and data manipulation during execution, ensuring robust system-wide Cloud security The proposed architecture has several potential uses, such as real-time monitoring of electric vehicle communication networks, anomaly detection in grid operations, and the creation of proactive defensive systems for critical infrastructure, such as power distribution nodes and charging stations, within interconnected smart communities. Validation of the efficacy of MIDF-MLA is accomplished through the utilisation of extensive simulation analysis. This investigation shows that MIDF-MLA can boost Cloud security, optimise resource allocation, and keep the system intact under several assault scenarios. This framework lays the platform for future advancements in electric vehicle protection within the broader context of smart grids.*

Keywords *- Intrusion Detection, Nonlinear, Machine Learning, Cloud security, Electric, Vehicles, Smart Grids, DDoS.*

1. Introduction

Authoritative or rule-based approaches are frequently utilised in implementing intrusion detection solutions for EVs in smart grids [1]. These systems can identify common dangers by comparing incoming data with a database of attack signatures or other predefined criteria, and then dangers can be identified [2]. Cyberattacks are still flexible, a major problem, particularly for smart grids with their massive and ever-changing distributed denial-of-service attack surface [3]. Because signatures do not always correlate with one another, information cloud security systems that rely on signatures are unable to recognise novel threats [4]. Although rule-based systems are flexible, they are quite setup-intensive and prone to false positives. When rule-based systems deviate from patterns, even harmless behaviours could be mistaken for hazardous ones [5]. The distributed and decentralised nature of smart grids makes it more challenging to use standard procedures compared to less dynamic and more centralised systems [6]. EV and smart grid components produce vast quantities of data, which overwhelms these systems and delays detection and response [7]. Adopting adaptive learning is uncommon in traditional systems, even if it is valuable in environments where denial-of-service attack vectors constantly appear [8]. In the absence of these measures, vital infrastructure may continue to be exposed, and the use of Advanced Persistent Threats (APTs) and other similar techniques by attackers to evade detection is becoming increasingly common [9]. When more powerful, adaptable, and scalable options are required, the shortcomings of conventional smart grid electric vehicle Cloud security become apparent [10].

A MIDF that makes use of robust nonlinear machine learning has been placed together to ensure the safety of EVs that are linked to the smart grid [11]. Dynamic and complex cyberattacks are challenging to foresee and detect; despite their benefits, nonlinear machine learning systems need a lot of high-quality training data to discriminate safe and dangerous behaviours [12]. Smart grids make data collection and organisation difficult; when considering EV communication protocols, grid topologies, and device and component heterogeneity, this becomes apparent [13]. Addressing nonlinear machine learning algorithm processing needs is another difficulty. These models may not be suited for real-time applications that demand rapid detection and response due to memory and processing constraints [14]. Advanced detecting systems are difficult to integrate into EV and smart grid network architecture due to interoperability and compatibility difficulties. The system is susceptible to dangers posed by both false positives and false negatives; an excessive number of the former can disrupt operations and reduce confidence in the computer system [15]. Because smart grids are decentralised and dynamic, the intrusion detection system must adapt to changing network conditions and entry sites. MIDF's smart grid applications need more research due to these constraints. A MIDF and robust nonlinear machine learning are two of several ways to secure smart grid-connected EVs. Advanced data augmentation methods improve training data sets, making models more accurate and resilient. Distributed computing and edge processing reduces real-time detection and reaction computer employment. Model performance is preserved via adaptive learning approaches through model upgrades depending on denial-of-service attack patterns. When traditional approaches are combined with machine learning, detection accuracy is improved, and the number of false positives is reduced.

1.1. Problem Definition

Detecting and combating sophisticated cyberattacks makes designing MIDFs that apply strong nonlinear machine learning to protect smart grid-connected EVs challenging. Smart grids are dynamic and scattered, real-time detection requires computational power, high-quality training data is needed, and detection accuracy and false positive and false negative rates must be balanced. The architecture is additionally required to be extensible and adaptable, and it can deal with evolving threats and work in tandem with smart grid and electric vehicle systems.

1.2. Objectives

OSmart grid EV cyberattacks like DDoS, spoofing, and data manipulation can be better detected with the help of a robust nonlinear machine learning model implemented in MIDF-MLA. Reducing the frequency of false positives via optimal optimization of the framework would enable efficient and reliable identification of true threats without stopping smart grid operations. Establishing a multi-stage architecture is essential for providing comprehensive, real-time monitoring and proactive protection measures for critical infrastructure inside interconnected smart communities. The results of the literature review are presented in Section 2. The second investigation, Enhancing Cloud Security in Electric Vehicles within Smart Grids, will be based on these results. The subject area is thoroughly examined in Section 3, which focuses on MIDF-MLA. The analysis that follows the presentation of the findings is located in Section 4 of this report. Section 5 includes the report's executive summary as well as its final recommendations.

2. Related Work

New cyberCloud security threats arise from these advances. Intrusion detection and system resilience methods using Machine Learning (ML) and Deep Learning (DL) models have been developed to address these threats. The suggested technique by Khan, I. A. et al. [16] makes use of a Multi-Stage Intrusion Detection Framework (M-SIDF) in conjunction with a deep learning-based bidirectional LSTM architecture for real-time intrusion detection in Intelligent Transportation Systems. The method achieves an accuracy of 98.88% on the UNSWNB-15 dataset and 99.11% on the automobile hacking dataset. Along with providing a summary of cyber risks and defence solutions, Rao, P. U. et al. [17] examine Machine Learning (ML) and Deep Learning (DL) techniques for improving smart grid cyberCloud security. Additionally, they demonstrate the efficacy of ML methods by means of an application study.

The TSKFS&MADRL technique is presented by Sepehrzad, R. et al. [18] as a means of analysing and improving the resilience of EVCS against cyberfires. In comparison to other technologies, it detects Foreign Direct Investment (FDI) 40% faster and achieves 7.33% reduced operation expenses. AlHaddad U et al. [19] propose a Hybrid Deep-Learning technique (H-DLA) using convolutional neural networks and recurrent gated units to detect attacks, including Distributed Denial of Service (DDoS), on smart grid communication. This approach achieves an accuracy of the system as high as 99.86%, yet real-time monitoring is not a challenge. Zibaeirad, A. et al. [20] discuss the applications of smart grid technology, address the issues of smart grid secrecy and examine the types of threats, strategies of use of the threats and the counter strategies centers on machine learning and blockchain. The paper resolves the problems encountered in the research and suggests further development of directions such as machine Learning Adversarial and Learning Models (LLMs). Bhadani U. et al. [21] suggested combining complex physical and cyber networks into a smart grid raises technical challenges. Due to its size, the future smart grid would need a more complex information and communication infrastructure than current electrical systems. With cutting-edge monitoring, regulating, and communication technology, smart grids provide a steady power supply, boost generator and distributor efficiency, and offer consumers options. An efficient, stable, and adaptable smart grid enhances electric power grid efficiency. This power system will be updated for safety, efficiency, environmental effects, and customer network management. The smart grid will be clarified in this survey.

Yang P. et al. [22] provided electric vehicles' rising in-car and inter-car connectivity may strain infrastructure. This essay will focus on electric vehicle cyberattacks and protect them from hackers by offering a secure and trustworthy intelligent framework. This study proposes a blockchain-based smart cloud computing and fuzzy machine learning strategy for cyber Cloud security analysis based on electric vehicle technology. This instance uses the smart grid integrated cloud computing model to monitor and transmit electric car data and the Fuzzy Adversarial Q-Stochastic model (FAQS) to assess unsafe activities. Data is encrypted and decrypted depending on role-based access control rules and the people who have access rights. Various cyber Cloud security data sets are tested for Cloud security rate, RMSE, quality of service, scalability, and energy efficiency. Gupta N et al. [23] provided that transportation is rapidly switching from fossil fuels to renewables. The new mobility idea comprises cars that store renewable energy and enable ecologically sustainable transportation. Cloud security risks rise as e-mobility infrastructure becomes more complex. Grids are important, crucial infrastructures that cyber attackers target. Technically, EVs and smart grids must communicate data. Smart grids must solve four major challenges to ensure eMobile charging Cloud security and privacy. Blockchain's trust-building technology can help the smart grid manage demand response and trade electricity efficiently and reliably.

Khalaf M et al. [24] focused on smart grid Cyber-Physical Cloud Security (CPS). ADNs are neglected in survey articles, which concentrate on smart grid transmission risks and problems. ADNs are being deployed rapidly, and cyber risks to power grids and critical infrastructures are rising. Thus, we decided to examine and survey the current CPS research for ADNs. The paper gives the first timely assessment of ADN CPS research on important operations and components. The cyber-physical components of each essential operation/component are examined. The problems and needs of communication protocols and standards are also discussed. ADN devices and sensors, including PMUs, smart meters, advanced metering infrastructure, and protective relays, are explored in depth for cyberCloud security. ADN application drivers and enablers such as microgrids, EVs, IoT, and smart homes are also studied. Industry-specific solutions are emphasized.

Aoudia M et al. [25] recommended that modern solutions must be put in place to prevent needless energy waste as the number of EVs is expected to expand along with the 3Ds—decarbonization, decentralization, and digitalization. EV charging frameworks in networks powered by renewable energy resources have been the subject of much research. Also, using blockchain technology to guarantee trading systems Cloud security and transparency have been getting a lot of attention lately. The intricacy of the problem has prevented several researchers from exploring how to put their answers into practice. Consequently, the purpose of this paper is to conduct an in-depth analysis of the current practical implementation and features of electric car charging systems that include blockchain technology. The MIDF-MLA detection and elimination of a large number of threats in the cyberspace of smart grids is the most efficient and least cumbersome compared to all other alternate techniques.

3. Proposed Methodology

The purpose of this paper is to enhance the Cloud security of smart grids with the introduction of EVs. The very nature of smart grids! The diversity of the networks and the particularism of mash networks that makes them non-flat and susceptible to more complex attacks influence their bolt-and-nut reliability and dependability enormously. MIDF-MLA employs a very accurate machine learning algorithm that employs the use of the growing set of features to adapt to new and growing threats, thereby increasing the proportion of correctly identified threats while decreasing that of false alarms. MIDF-MLA delivers end-to-end coverage and monitoring in real-time on EV communication network and grid operation, enhancing the Cloud security of the system through a multi-tiered domain. The improvement of the comprehensive framework is thoroughly examined and validated with the help of simulation analysis that highlights the efficiency of the framework in resource allocation, system protection, and communication Cloud security during denial-of-service attack situations.

3.1. Methodology of the Research

The MIDF-MLA was developed because of the study's efforts to build a strong IDS specifically for smart grids' EVs. Cyberattacks, including DDoS, spoofing, and data manipulation, are all part of the framework's multi-stage design. To guarantee effective threat identification and mitigation throughout different phases of the framework, the design uses a nonlinear machine learning model that aims to improve detection accuracy while decreasing false positives.

4. Contributions

4.1. Contribution 1: Framework Development for Multistage Intrusion Detection

A progressive intrusion detection specialist applied in the context of Smart grids with a focus on Electric Vehicles. This methodology makes the system more robust by systematizing and limiting the cyber threats at multiple entry points in the network and smart grid operational ecology. The methodology achieves total protection from any emerging cyber threats by eliminating any possible vulnerability throughout the whole operational process. The application of a multi-stage procedure makes it possible to design a Cloud security mechanism that has multiple layers. This mechanism aims to defend against deep threats and guarantee the operability of the energy distribution and the integral work of the vehicles within the smart grid.

$$Ev_{n-1} - mn_y + W_{qr} = \frac{3}{1-u} * \partial(y-k),$$
$$y \equiv S, u+1 < 0 \qquad (1)$$

The system state $\frac{3}{1-u}$ from the previous stage W_{qr} is represented by Equation (1) Ev_{n-1}; the model's dynamic parameter is indicated by mn_y, and outside forces $\partial(y-k)$ or weights are reflected by $y \equiv S, u+1$.

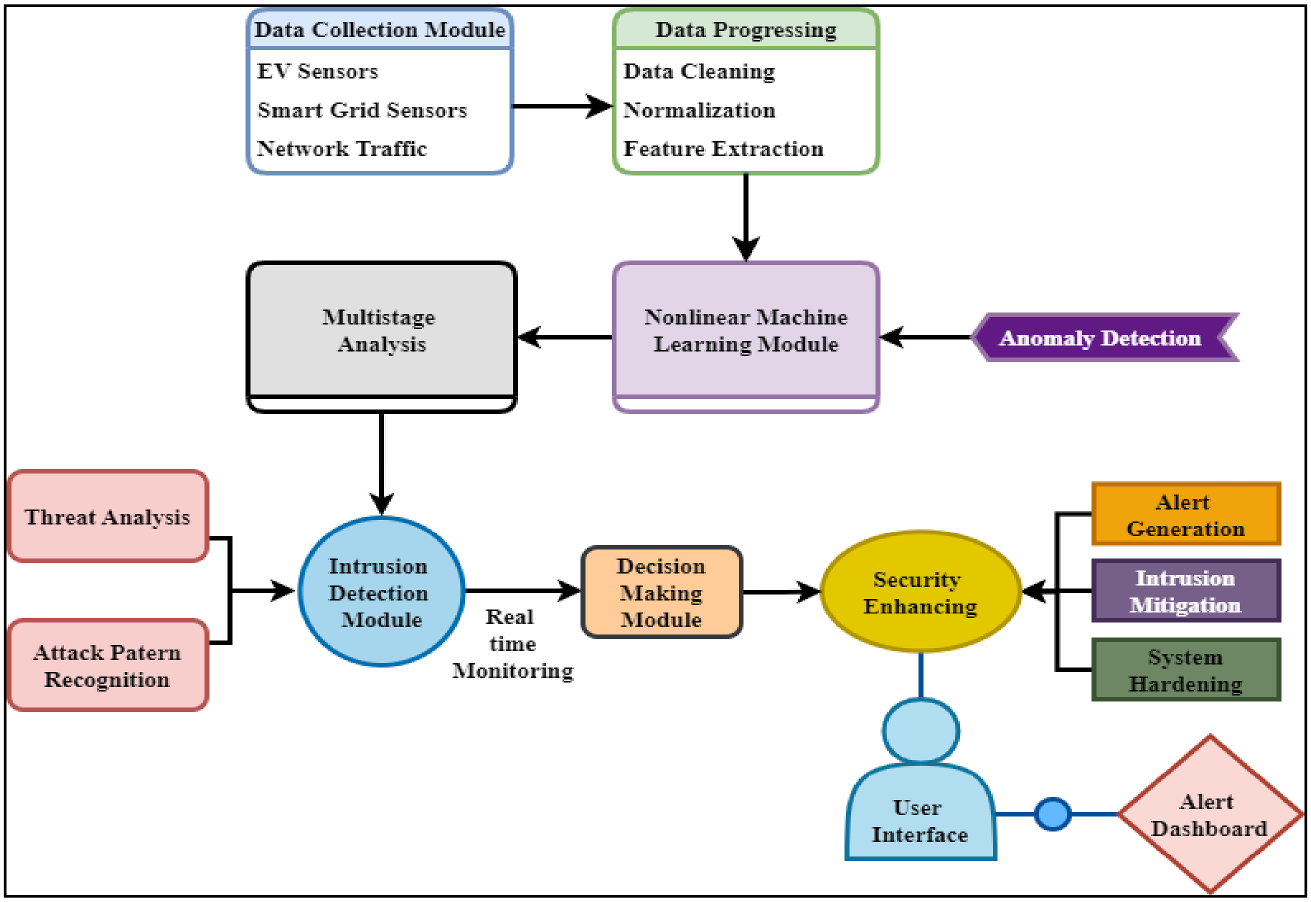

Fig. 1 Structure of intrusion detection framework utilising machine learning approach

Figure 1 shows the structure of the MIDF-MLA to improve the Cloud security of EVs interconnected with smart grids. The first stage involves the primary function of the data collection module, which is to collect data from several sources, such as smart grid sensors, electric vehicle sensors, and network traffic concurrently. The processing of data involves the tasks of cleaning, standardizing, and extracting characteristics. Both the multistage analysis module and the Nonlinear machine learning module operate simultaneously with the preprocessed data. Although the nonlinear machine learning module improves the system's capacity to detect anomalies, the multistage analysis approach is responsible for identifying and classifying several stages of possible threats. The Intrusion Detection Module combines algorithmic techniques for threat analysis and attack pattern recognition to detect possible intrusions. The Decision-making module determines suitable measures, such as raising alarms, minimizing intrusions, or securing the system after discovery. These operations are sent via a user interface and displayed on an alert dashboard, leading to an improvement of system Cloud security through the Cloud security enhancing procedure.

$$f(y,0) = Z_o(y-1), y \equiv Z\big(f(mkn^{-1} * q)\big) \quad (2)$$

Equation (2), in which the constant $f(y,0)$ and the parameter Z_o affect $(y-1)$. This indicates a recursive dependence as y is decided by another function of variables Z, such as $f(mkn^{-1} * q)$.

$$d_f(n-1) = \frac{2w}{(4\forall) * (5^{n-1}!)} * F_{d(k-1p)} + Q_{w(p-1)} \quad (3)$$

The detection function d_f is modeled by Equation (3), which depends complexly on variables such as weights $n-1$, a factorial function, and values $\frac{2w}{(4\forall)*(5^{n-1}!)}$.

It illustrates how the suggested MIDF-MLA approach exactly modifies its detection capabilities $F_{d(k-1p)}$ via complex calculations $Q_{w(p-1)}$ involving many elements.

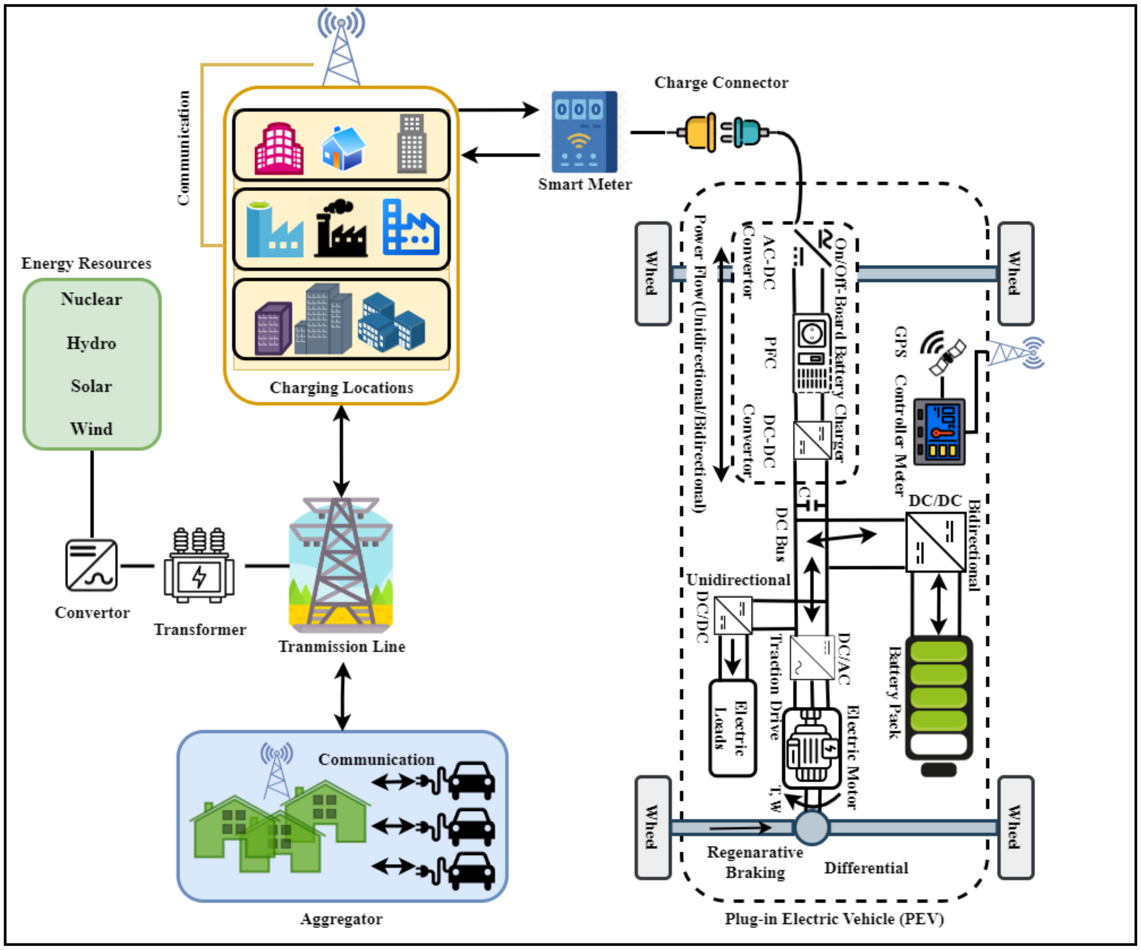

Fig. 2 EV charging-dispatch and vehicle-to-grid technologies

Figure 2 provides a high-level perspective of the smart grid infrastructure. It emphasizes the connection between the needs of the industrial and urban areas and the integration of various energy sources. Commercial, residential, and industrial load centers are connected to the electrical infrastructure by a grid network managed by communication systems. The electric motor in an EV gets its power from the battery pack through traction drivers, AC/DC converters, and DC/DC converters. Regenerative braking is possible because of the bidirectional and unidirectional energy flow. The figure shows the role of GPS and onboard meters in facilitating efficient data transmission between the grid and EVs. It highlights the importance of both wired and wireless communication. The system's integration of smart communication and renewable energy sources improves the grid's reliability, efficiency, and Cloud security [27], in addition to fulfilling the primary objective of a strong and secure smart grid design.

$$m_k(U_{kp-1}) = B_{kp}\left(y\big(Mr_{(y-tp)}\big)\right) + \left(Zer_{(p-kt)} * Y^{k-1}\right) \quad (4)$$

The Equation (4) wherein the functions $m_k(U_{kp-1})$, B_{kp}, and $Zer_{(p-kt)}$determine Y^{k-1}. This demonstrates the use of intricate, nonlinear mathematical $y\big(Mr_{(y-tp)}\big)$ models to capture dependencies and interactions in the data, which is consistent with the suggested MIDF-MLA approach.

$$Y_{k(t-1)} = B_{jk}\left[fg_{n-1} + Y\left(xv(ct - pk)\right)\right] - Z_{p(y-x)} \quad (5)$$

With the help of historical values $Y_{k(t-1)}$, a recursive function B_{jk}, and a correction factor fg_{n-1}, Equation (5) depicts the dynamic development of $\left(xv(ct - pk)\right)$.

This illustrates the adaptive nature of the MIDF-MLA, which uses complex interconnections Y and historical data $Z_{p(y-x)}$ to improve intrusion detection and strengthen system resilience against changing cyber threats.

4.2. Contribution 2: Integration of Nonlinear Machine Learning Techniques

MIDF-MLA with nonlinear machine learning techniques. The solutions are developed to handle cyberattacks that are complex and constantly evolving. The robust, non-linear model increases intrusion detection accuracy by learning from new threats and producing fewer false positives. The ability to adapt is essential to keep the smart grid secure and reliable as it improves. By integrating these strategies, the MIDF-MLA is able to effectively address evolving threat patterns, hence establishing a proactive defensive mechanism inside the smart grid system.

$$Bk_{pt} = \frac{M[xy - pk]}{Erv^{k-1}} + \left(y_{jk} - P(k) * Z^2Qn(1 - p)\right) \quad (6)$$

Several nonlinear terms, including Bk_{pt}equation variables $y_{jk} - P(k)$, Z^2Qn are involved. This illustrates how the MIDF-MLA models system behavior $(1 - p)$ and improves detection techniques by using complex mathematical connections.

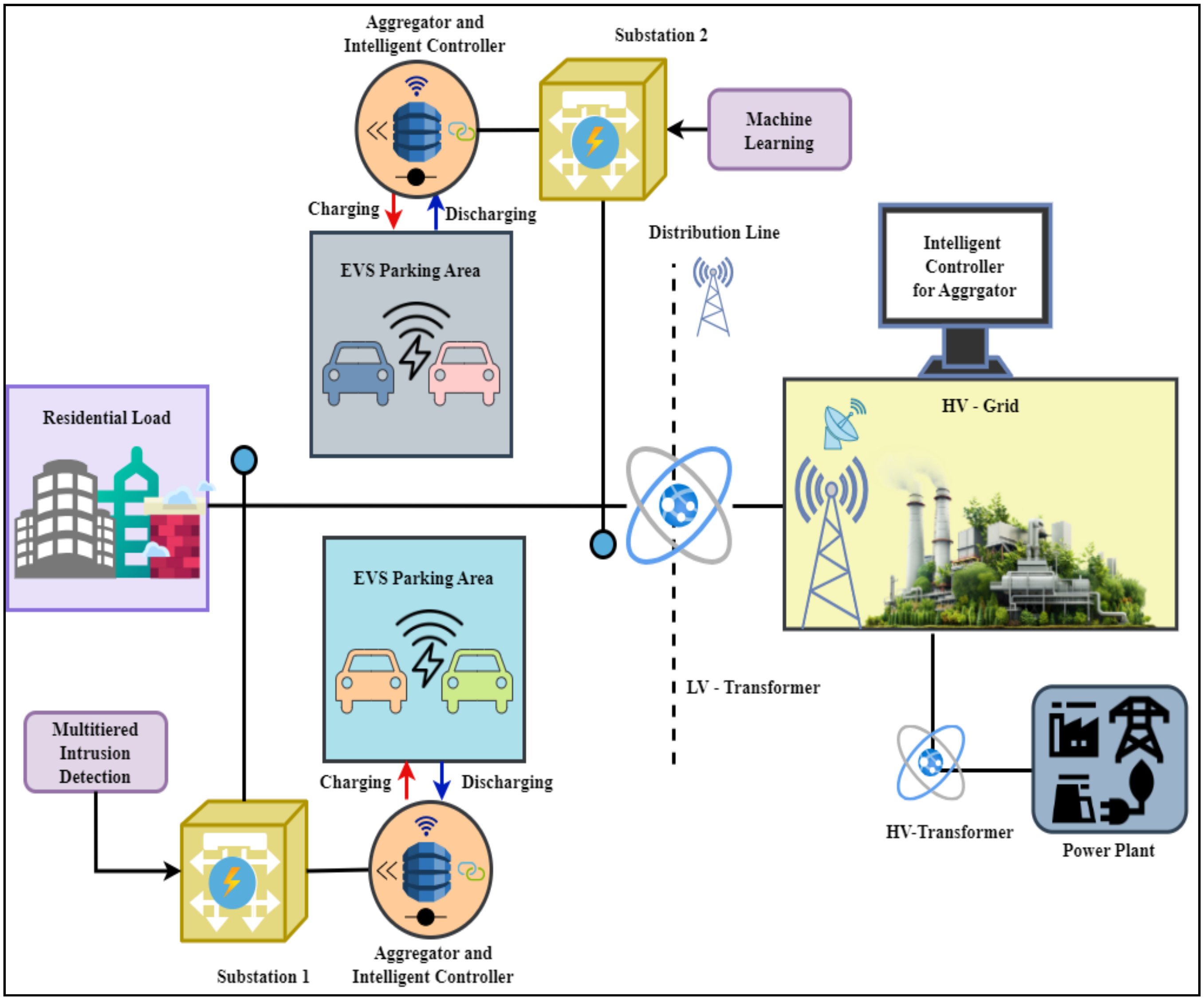

Fig. 3 Smart charging and discharging using multitiered intrusion detection

Figure 3 illustrates a smart grid infrastructure that incorporates EVs in parking spaces, with an emphasis on providing safe energy distribution and management using a Multitiered Intrusion Detection system. The EVs inside the parking areas are connected to the high-voltage grid via an intelligent controller for the Aggregator. This controller effectively controls and improves the energy transfer between the grid and residential loads. Multitiered Intrusion Detection ensures the Cloud security of communication between the grid, EVs, and residential loads, while Machine Learning significantly improves the system's capacity to react to unexpected threats. The residential load represents the consumer segment of the power system, which is responsible for the distribution of energy. The parking areas and the grid engage in bidirectional communication, which is carefully monitored to detect any cloud security breaches, ensuring accurate and powerful operations. The integrity and efficiency of the energy distribution network are heavily dependent on the continuous monitoring and anomaly detection of the whole system in this developing smart grid environment.

$$Es_{j-k} = \{v \equiv B: (j,k) + E^{k-1}(k-1)\} \qquad (7)$$

Equation (7) characterizes a set in which the connection between variables Es_{j-k} and $v \equiv B$ defines E^{k-1}. The complex used emphasized the multifactor $(k-1)$ based on the convey sets (j,k) depending on the MIDF-MLA consistent techniques with representation.

$$M(y-z) = E(nm) - N(Y) = \left[M_{k=1} + B_{np} - R_f(n-1)\right] \quad (8)$$

The connection shown by Equation (8) is one in which $M(y-z)$ it is a function of many variables, and distinct impacts are captured by the terms $E(nm)$, $N(Y)$, and the sum of $M_{k=1}$, B_{np}, and $R_f(n-1)$.

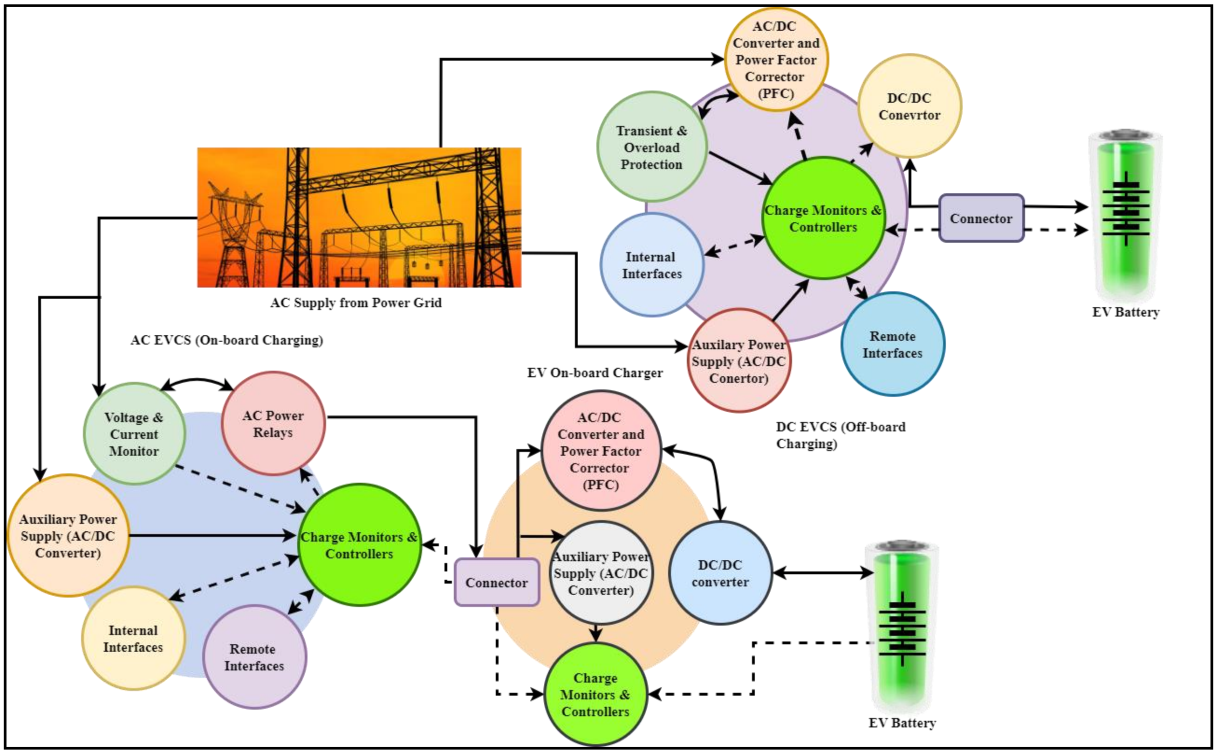
AC/DC Converter and Power Factor Corrector (PFC)
DC/DC Conevrtor
Transient & Overload Protection
Charge Monitors & Controllers
Connector
Internal Interfaces
Remote Interfaces
Auxilary Power Supply (AC/DC Conertor)
EV Battery
AC Supply from Power Grid
AC EVCS (On-board Charging)
EV On-board Charger
DC EVCS (Off-board Charging)
Voltage & Current Monitor
AC Power Relays
Auxiliary Power Supply (AC/DC Converter)
Charge Monitors & Controllers
Connector
Internal Interfaces
Remote Interfaces
AC/DC Converter and Power Factor Corrector (PFC)
Auxiliary Power Supply (AC/DC Converter)
DC/DC converter
Charge Monitors & Controllers
EV Battery

Fig. 4 Typical EVCS cyber-physical layer schematic

Figure 4 shows the smart grid layout, with the many parts that safeguard the electric vehicle charging system and manage electricity efficiently. The operation's principal control units that monitor charging are the charge monitors and controllers. Power conversion and stabilisation operations are performed by the AC/DC Converter and Power Factor Corrector (PFC), while the DC/DC Converter efficiently controls the power distribution within the vehicle. The Auxiliary Power Supply (AC/DC Converter) offers additional energy assistance to ensure the system's reliability. Voltage and current monitors control the current and voltage that flows through the system to protect a system from power surges and interruptions.

While AC power relays maintain the connections to power circuits, remote interfaces communicate with other systems. The internal Interface enables communication between internal components. The charging process terminated after the connector creates a secure physical link between the electric vehicle and the charging station.

$$A^u * M_{z-1} = \frac{1}{2} * b_{kp}\left(sq_{(w-1)} * M_{z-1}\right) + \left(Q_{wz-2}\right) \quad (9)$$

The exponential term is set to be linked M_{z-1} with the functions A^u based on itself based on the given Equation (9). The relationship $\frac{1}{2} * b_{kp}$ is set to define with the feedback $, sq_{(w-1)}$ based on the MIDF-MLA depending on the danger levels M_{z-1} set with the dynamic adaptation Q_{wz-2}, and the system-enabled state.

$$v_b(k-1) = M_2Y(v-kp) + F^{v-1}\left(zy(p-1)\right) \quad (10)$$

Equation (10), has an extra term involving $M_2Y(v-kp)$, where F^{v-1} is determined by the product of zy and $p-1$. The cyber threats are sets based on the relational recursive values based on the factors that are non-linear based on the utilization v_b and illustration. The equation is set with the functionalities based on the MIDF-MLA based on the techniques $(k-1)$.

4.3. Contribution 3: Comprehensive Simulation Validation

Contribution 3 validates the MIDF-MLA framework using simulations while evaluating it in detail. To determine how well the framework strengthens Cloud security improves resource allocation, and preserves system integrity, the validation process includes substantial testing across multiple attacks (DDoS) scenarios.

The simulations show that MIDF-MLA has the capacity to effectively identify and address potential dangers in real time, consequently ensuring the stability and durability of smart grid operations.

The validation demonstrates the framework's practical usability for real-time monitoring and anomaly detection in electric vehicle communication networks, illustrating its potential for extensive implementation in smart grid scenarios.

$$F(y,z) = M_1(yz) - M_z(x-pk) + E_0(z,yp) \quad (11)$$

The function $F(y,z)$ is described by the equation, which E_0 adds a component and (yz) indicates distinct terms involving z, yp, and other variables. The accuracy analysis M_z and the detection rate M_1 is based on the approach depending on the MIDF-MLA based on the behavior over a complex system based on the interactions with the emphasized integration.

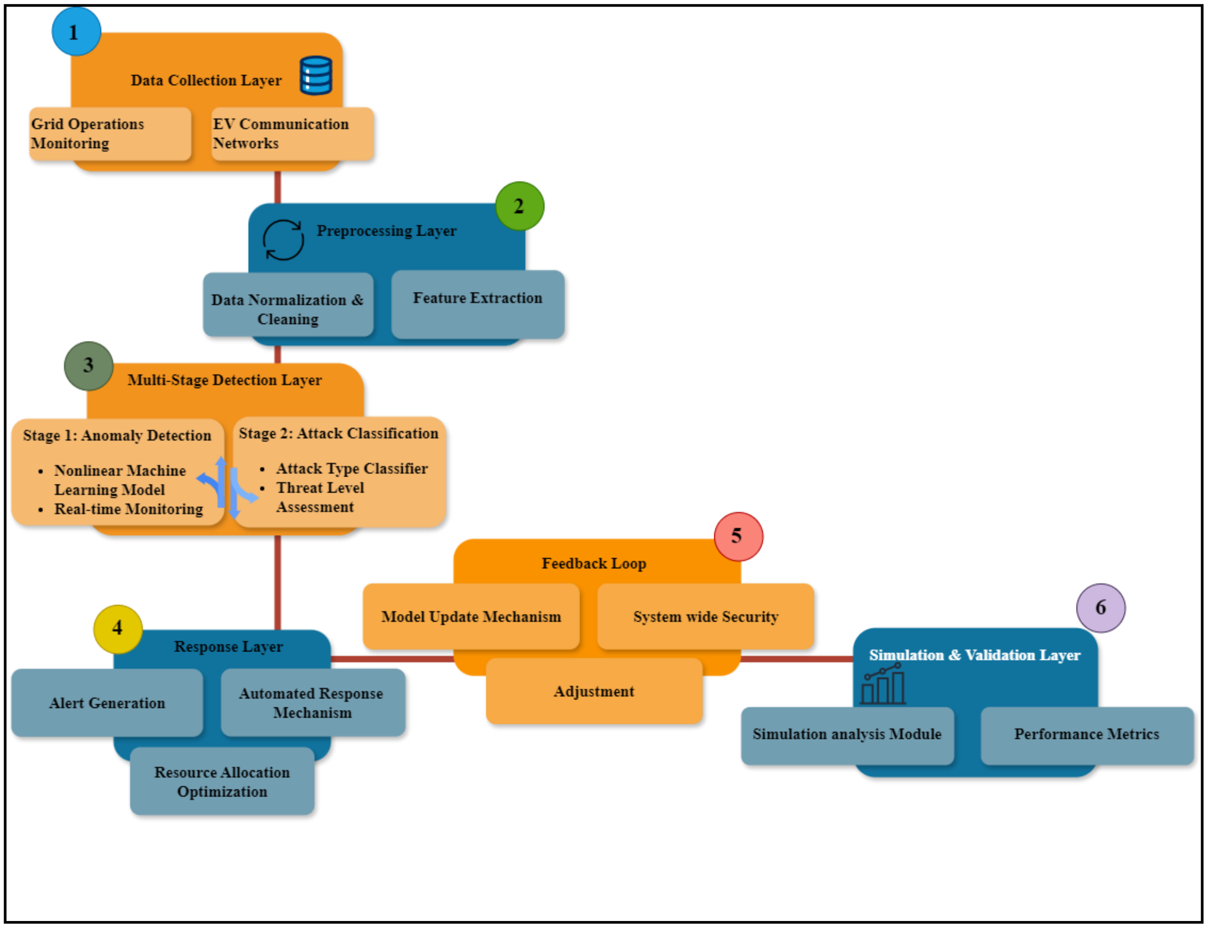
1
Data Collection Layer
Grid Operations Monitoring
EV Communication Networks
2
Preprocessing Layer
Data Normalization & Cleaning
Feature Extraction
3
Multi-Stage Detection Layer
Stage 1: Anomaly Detection
Nonlinear Machine Learning Model
Real-time Monitoring
Stage 2: Attack Classification
Attack Type Classifier
Threat Level Assessment
5
Feedback Loop
Model Update Mechanism
System wide Security
Adjustment
4
Response Layer
Alert Generation
Automated Response Mechanism
Resource Allocation Optimization
6
Simulation & Validation Layer
Simulation analysis Module
Performance Metrics

Fig. 5 Process of MIDF-MLA

Figure 5 illustrates the MIDF-MLA to improve cyberCloud security in EVs in smart grids. The process begins with the data collection layer, which collects data from both grid operations monitoring and EV communication networks. The data is processed in the preprocessing layer, which includes data normalization, cleaning, and feature extraction to help prepare it for analysis.

The multi-stage detection layer consists of two stages: anomaly detection, which utilizes nonlinear machine learning models for monitoring in real-time, and attack classification, which utilizes an attack type classifier and threat level assessment to detect and identify DDoS attacks. Response layer acquires control of alert generation, automated response mechanisms, and resource allocation optimization to efficiently handle the identified threats. The Feedback loop ensures constant system improvement via model update mechanisms and modifications to preserve system-wide Cloud security. Finally, the simulation and validation layer uses a simulation analysis module and performance metrics to confirm and improve the performance of the framework, therefore ensuring its adaptability and dependability in real-world scenarios.

$$Z_1(y-z) = \frac{1}{4p}\left(\left|\left|Y_{p-1} + z_{q(nk)}\right|\right| - e_1\right) \quad (12)$$

Equation (12) illustrates the absolute variation between terms involving $Z_1(y-z)$, and a constant Y_{p-1}, scaled by $z_{q(nk)}$, affects e_1. The system latency analysis is set with procedures dealing with the technique modified $\frac{1}{4p}$ with the MIDF-MLA based on the modified threshold detection, where the user activity is set to be determined by the activity of a system.

$$M_x(yz) = \partial\beta(v - mn^{b-1}) + \left|\left|y_{s-1} + z_{kp}\right|\right| \quad (13)$$

The formula connects M_x to the absolute value of the sum $\partial\beta$ and v, as well as the partial derivative y_{s-1} of a function involving z_{kp}. The robustness analysis is determined with the parameter detection (yz) with the improved based on the relationships are defined with the intricates mn^{b-1} based on the absolute values and the deviations.

$$g_k^{1-p} = \forall \left|\left|R_{f-1} * Y_{qw}\right|\right| - e_f + \left(y_{q-1}, zp_{n-1}\right) \quad (14)$$

With the constant $e_f$and extra terms involving g_k^{1-p} and $\forall$, the equation expresses R_{f-1} as a function of the absolute value of e_f. The scalability analysis of the system is based on the technique based on the MIDF-MLA based on the consistency y_{q-1} depending on the account of the system configuration zp_{n-1} based on the risk.

$$Pk_{n-1} = b_0 + ||z_{vc} - Np(q-w) + \left(V_b - A_{cp}\right) \quad (15)$$

The formula is composed of the absolute value of a complicated expression including Pk_{n-1}, and b_0, as well as a constant z_{vc}. This illustrates how the MIDF-MLA approach models $Np(q-w)$ and modifies detection thresholds $V_b - A_{cp}$ using similar computations on resource efficiency analysis.

The proposed method improves the level of cyberCloud security in smart grids, specifically by including EVs. It uses a powerful, non-linear machine learning algorithm to adapt to new and evolving cyber threats, resulting in improved accuracy in detecting such threats and minimizing false positives. The multi-stage design of MIDF-MLA provides extensive Cloud security coverage for both EV networks and grid operations. After being thoroughly tested in simulations, MIDF-MLA efficiently improves the allocation of resources, preserves the integrity of the system, and strengthens Cloud security. As a result, it is well-suited for monitoring and detecting anomalies in real-time in smart grid scenarios.

Research Procedures: The investigation was carried out according to a predetermined protocol that included many essential steps. A simulation environment was set up to mimic EV activities inside smart grids, including cyberattack scenarios after the MIDF-MLA framework was built. We were able to gauge the framework's efficacy by analyzing data from these simulations, which included both typical operations and assault scenarios. Using this data, the MIDF-MLA's integrated machine learning model was trained and evaluated throughout the framework's phases to see how well it performed.

5. Results and Discussion

Within smart grids, the MIDF-MLA is intended to improve the safety of EVs; for the purpose of this research, the performance of MIDF-MLA is evaluated across a number of different aspects, such as detection rate, system latency, resilience, scalability, and resource efficiency. Through the incorporation of nonlinear machine learning techniques, the MIDF-MLA system intends to provide full protection against sophisticated cyberattacks while simultaneously preserving the integrity of the system and optimising the utilisation of resources.

Analyzing Data: To assess how well the MIDF-MLA worked, data analysis was carried out using a sequential approach. Preprocessing, which included cleaning and normalizing the raw simulation data, was done to guarantee that the machine-learning model was fed high-quality input. The performance indicators used to evaluate the model's ability to identify different attack types with few false positives. Through simulation research, we tested the framework's capacity to keep the system intact and optimize the allocation of resources in the face of assault scenarios. To further demonstrate MIDF-MLA's benefits in detection accuracy, reaction speed, and system resilience, the findings were further compared with pre-existing IDS models.

Dataset description: The multi-dimensional CIC EV charger assault dataset 2024 (CICEVSE2024) is useful for cyberCloud security research on EV charging stations. EVSE power usage, network traffic, and host activities under benign and attack scenarios are included [26]. Reconnaissance, DoS, Backdoor, and Cryptojacking are discussed. Statistics and machine learning for behavioral profiling and anomaly identification are possible with the dataset. Attack kinds, system states (Idle, Charging), and interfaces (OCPP, ISO15118) are labeled in the dataset.

Table 1. Environmental and simulation parameters

Parameter	Description
Simulation Environment	MATLAB/Simulink, Python with Scikit-learn, TensorFlow, and Keras for model training and evaluation
Dataset	EVSE Dataset 2024 from the Canadian Institute for CyberCloud security, containing Electric Vehicle Supply Equipment (EVSE) communication data within smart grids
Dataset Size	Approximately 100,000 data points with features such as charging session details, vehicle identification, network traffic, and operational status
Feature Selection Method	Recursive Feature Elimination (RFE) with cross-validation
Training/Test Split	80% training, 20% testing
Attack Scenarios	- Denial of Service (DoS) - Man-in-the-Middle (MitM) - Spoofing attacks - False data injection
Intrusion Detection Methods	- Signature-based detection - Anomaly-based detection using clustering (e.g., K-means, DBSCAN) - Hybrid detection approach
Model Training	Supervised learning with labeled attack scenarios and normal operation data
Simulation Duration	24 hours of simulated time with different phases of grid load, vehicle charging/discharging, and communication patterns
Hardware Specifications	- CPU: Intel Core i7 or higher - GPU: NVIDIA GTX 1080 Ti or higher for deep learning model acceleration - RAM: 32 GB
Software Libraries	- Scikit-learn - TensorFlow - Keras - NumPy - Pandas - Matplotlib
Hyperparameters	- SVM (C=1.0, Gamma=0.1) - Random Forest (n_estimators=100) - Neural Networks (LSTM units=128, batch size=64, epochs=50)
Noise and Disturbance Handling	Gaussian noise addition to simulating sensor inaccuracies and communication disturbances
Communication Protocols	Controller Area Network (CAN) protocol, Modbus, TCP/IP for vehicle-to-grid (V2G) communication
Cloud security Measures	- Encryption (AES-256 for data in transit) - Key Management for secure communication - Blockchain for logging and integrity verification

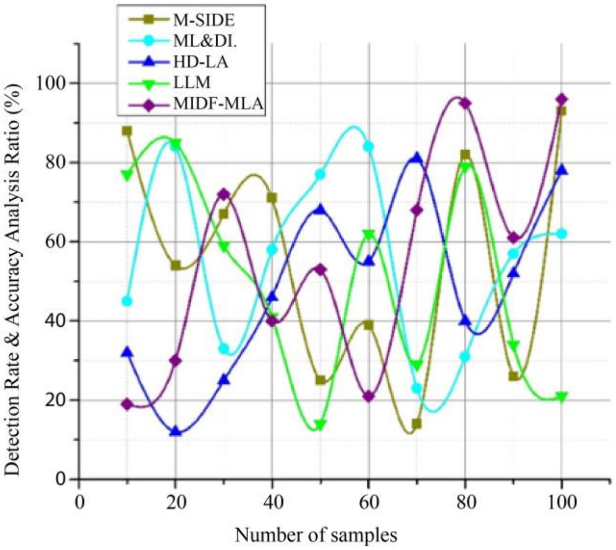

Fig. 6 Detection rate and accuracy analysis

In Figure 6, the MIDF's ability to protect EVs in smart grids relies on its detection rate and accuracy, which are increased by its nonlinear machine learning technique. MIDF-MLA's essential nonlinear machine learning model detects simple to complex attack vectors. Using simulations to train the framework could increase its detection rate and catch more hostile acts than earlier methods. Despite efforts, intrusion detection systems may produce false positives and negatives. MIDF-MLA limits false alerts; therefore, significant threats may be defended against, the system remains intact, and resources are optimally implemented. For complete coverage, the multi-stage architecture uses several levels of analysis adapted to individual attackers co; consequently, detection accuracy has improved, producing 96.7%. Due to its high detection rate and precision, MIDF-MLA is a great solution for EV safety in the complex smart grid ecosystem and protects the system against several cyberattacks.

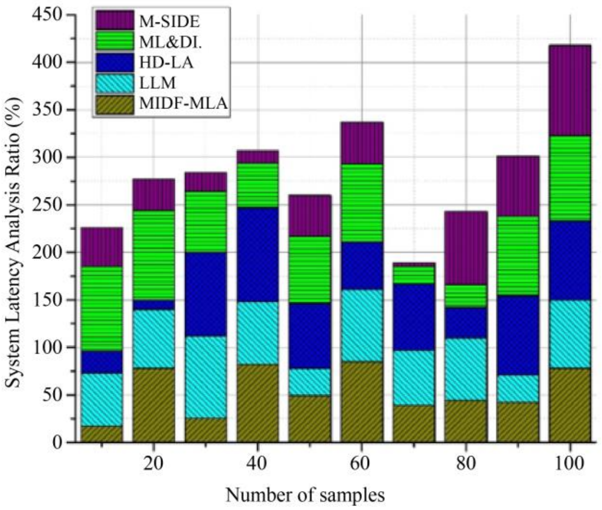

Fig. 7 System latency analysis

Assessing the MIDF using a strong nonlinear machine learning algorithm to protect EVs in smart grids requires considering system latency. In the above Figure 7, this definition of latency refers to the time between detecting a threat and reacting. The computing needs of nonlinear machine learning algorithms may cause latency in MIDF-MLA's multi-stage design despite its initial goal of full Cloud security through multi-layer data analysis. Detecting complex assault patterns requires a lot of computing resources. When confronted with massive amounts of real-time data from electric vehicles and smart grid networks, this becomes apparent. Latency is reduced by distributed computing and edge processing, and this approach lets several nodes near the data source compute. Reducing data transmission and processing time speeds up danger detection and response. Finally, MIDF-MLA's adaptive learning methods are adapted to the biggest threats. With this, any Cloud security violation will be addressed instantly. For smart grid reliability and integrity, MIDF-MLA prioritises quick Cloud security measures, producing 95.9%. Even though complicated frameworks like this have system slowness.

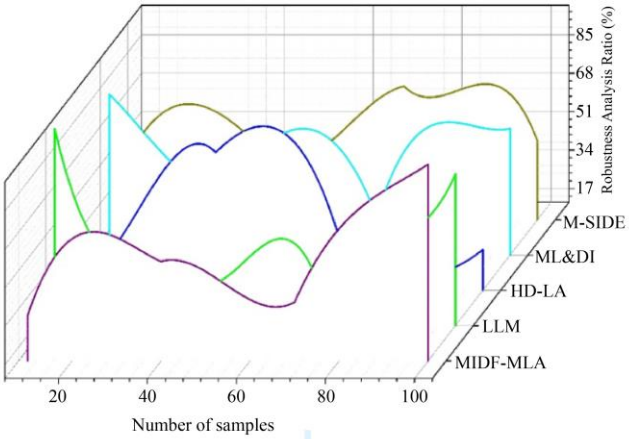

Fig. 8 Robustness analysis

Figure 8 shows that MIDF needs to be examined using robust nonlinear machine learning to defend smart grid EVs; this test evaluates the framework's resilience to attacks and network issues. MIDF-MLA tackles complex and dynamic threats with nonlinear machine learning. Large-scale resilience tests simulate DDoS, spoofing, data manipulation, and other cyberattacks.

The multi-stage architecture of MIDF-MLA adds several detection layers to address specific network Cloud security issues to increase robustness. The multi-tier design helps the following steps identify and respond to dangers even if a step is compromised. Adaptable learning makes the framework robust against new threats, producing 98.2%. MIDF-MLA protects electric vehicles in smart grid situations despite smart grids' dynamic and distributed nature and DDoS attacks.

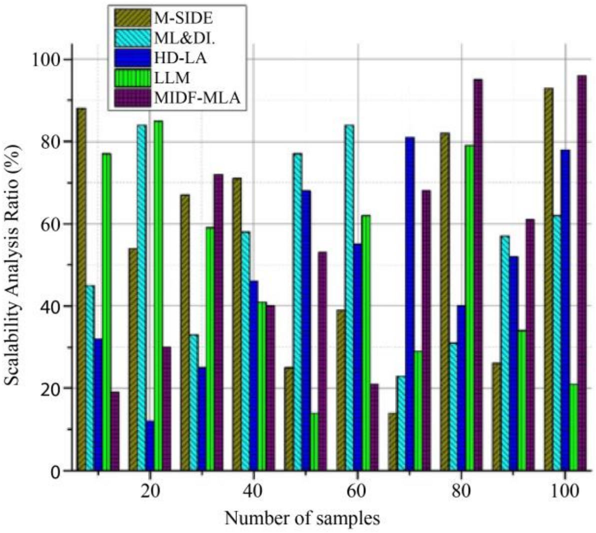

Fig. 9 Scalability analysis

Scalability investigation using an effective nonlinear machine learning technique determines if the MIDF can satisfy EV smart grid development needs. Because smart grid and EV components generate complex data, scalability is essential. In Figure 9, MIDF-MLA scales well by spreading computing across layers and nodes due to its multi-stage design. As the network grows and more data is processed, this method keeps everything working smoothly. Due to distributed computing and edge processing, MIDF-MLA's nonlinear machine learning model can dynamically allocate resources to changing data loads and network topologies. This distributed method decreases latency and ensures consistency in all operational settings while improving the system's ability to manage large-scale deployments, and adaptive learning lets MIDF-MLA expand. Detection algorithms are upgraded and improved to tackle new threats. MIDF-MLA's scalability makes it perfect for electric vehicles and smart grids, producing 96.9%. As a result of this action, one can ensure that the network will continue to expand while maintaining a high level of integrity and effectiveness.

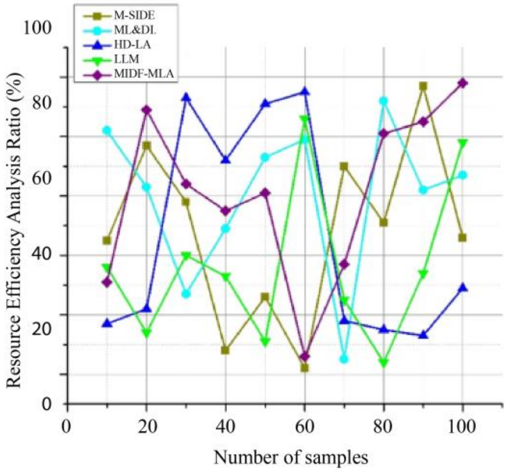

Fig. 10 Resource efficiency analysis

The MIDF resource efficiency is examined by utilising robust nonlinear machine learning. The present research examines operational and computational resource utilisation to protect smart grid-connected EVs. In the above Figure 10, through the integration of many processes, MIDF-MLA optimises resource utilisation. The multi-stage architecture allows processing workloads to be distributed over multiple levels, reducing component pressure and optimising computational resources. Nonlinear machine learning algorithms are computationally efficient with data purification and dimensionality reduction. Distributed computing and edge processing increase resource efficiency while this optimiser balances processing requirements and accuracy. By evaluating data at the source, MIDF-MLA reduces central data transfer and processing and adapts resource allocation to changing network conditions and real-time danger detection via adaptive learning. System performance, operational expenses, and energy savings are improved by this dynamic technique by 98.1%. MIDF-MLA secures EV smart grids while optimising resource utilisation with these resource-efficient technologies, making the network sustainable and scalable. The evaluation of MIDF-MLA reveals that it is highly effective in protecting electric vehicles within smart grids. In general, MIDF-MLA emerges as a system that is both dependable and effective for protecting electric vehicles in smart grid contexts.

6. Conclusion

To improve the safety of EVs connected to smart grids, we presented the MIDF-MLA in this paper. Multiple cyberattack vectors, including DDoS, spoofing, and data manipulation, are successfully addressed by the proposed framework's multi-stage design and strong nonlinear machine learning model. Results from our comprehensive simulation study show that MIDF-MLA optimizes resource allocation, keeps the system intact, and greatly increases detection accuracy across a range of assault scenarios. The findings support the idea that MIDF-MLA may improve the safety of vital infrastructure in linked smart communities, which will lead to smart grid operations that are more robust. The architecture guarantees the quick detection and mitigation of real threats without affecting key services by decreasing false positives. There are a number of promising new directions for future study and development. To begin, the IDS's flexibility and accuracy might be further improved with the use of more sophisticated machine learning methods like deep learning and reinforcement learning. Investigating these methods might lead to a more robust system for identifying ever-changing cyber dangers. A more all-encompassing Cloud security solution for the ecosystem might be achieved by extending the framework's coverage to include additional smart grid components like Distributed Energy Resources (DERs) and IoT devices. To further confirm the framework's efficacy under actual situations, future studies might also concentrate on implementing and testing it in live smart grid scenarios. Finally, adding self-learning capabilities to MIDF-

MLA might make the system resilient in the long run by automatically adjusting to new threats as smart grids and EV networks change. Contributing to the creation of autonomous, intelligent Cloud security systems for future smart infrastructures, this process will include continual learning from fresh data and real-time feedback.

Author Contribution

Selvakumari S, Prabhakar K, and Selvakumaran S have conceptualized the study, developed the methodology, and supervised the work. This author led the design and implementation of the machine learning models and played a significant role in writing the manuscript., Mythili Nagalingam, C. Tamilselvi, Mohanaprakash T A was responsible for data analysis, the design and deployment of the system, and the development of algorithms; Mohanaprakash T A also assisted in manuscript preparation and editing and contributed to the literature review and background research, coordinated research activities across different institutions, and supported manuscript drafting and proofreading.

References

[1] Hossein Mohammadi Rouzbahani, Hadis Karimipour, and Lei Lei, "Multi-Layer Defense Algorithm against Deep Reinforcement Learning-Based Intruders in Smart Grids," *International Journal of Electrical Power & Energy Systems*, vol. 146, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Muzun Althunayyan, Amir Javed, and Omer Rana, "A Robust Multi-Stage Intrusion Detection System for In-Vehicle Network Cloud Security Using Hierarchical Federated Learning," *Vehicular Communications*, vol. 49, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Mohammad Ali Sayed et al., "Grid Chaos: An Uncertainty-Conscious Robust Dynamic EV Load-Altering Attack Strategy on Power Grid Stability," *Applied Energy*, vol. 363, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Hamad Naeem, Farhan Ullah, and Gautam Srivastava, "Classification of Intrusion Cyber-Attacks in Smart Power Grids Using Deep Ensemble Learning with Metaheuristic-Based Optimization," *Expert Systems*, vol. 42, no. 1, pp. 1-25, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[5] B. Prabadevi et al., "Deep Learning for Intelligent Demand Response and Smart Grids: A Comprehensive Survey," *Arxiv*, pp. 1-25, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Mohammad Ghiasi et al., "A Comprehensive Review of Cyber-Attacks and Defense Mechanisms for Improving Cloud Security in Smart Grid Energy Systems: Past, Present and Future," *Electric Power Systems Research*, vol. 215, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Parya Haji Mirzaee et al., "Smart Grid Cloud Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures)," *IEEE Access*, vol. 10, pp. 52922-52954, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Boyu Wang et al., "AI-Enhanced Multi-Stage Learning-to-Learning Approach for Secure Smart Cities Load Management in IoT Networks," *Ad Hoc Networks*, vol. 164, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sudha Anbalagan et al., "IIDS: Intelligent Intrusion Detection System for Sustainable Development in Autonomous Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 15866-15875, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Reza Sepehrzad et al., "Enhancing Cyber-Resilience in Electric Vehicle Charging Stations: A Multi-Agent Deep Reinforcement Learning Approach," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 11, pp. 18049-18062, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Li Yang, Abdallah Moubayed, and Abdallah Shami, "MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616-632, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Tasneem A. Awaad et al., "Detecting Cyber Attacks in-Vehicle Diagnostics Using an Intelligent Multistage Framework," *Sensors*, vol. 23, no. 18, pp. 1-30, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Andrej Novak, and Alexei Ivanov, "Network Security Vulnerabilities in Smart Vehicle-to-Grid Systems Identifying Threats and Proposing Robust Countermeasures," *Journal of Artificial Intelligence and Machine Learning in Management*, vol. 7, no. 1, pp. 48-80, 2023. [Google Scholar]

[14] Irfan Ali Kandhro et al., "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," *IEEE Access*, vol. 11, pp. 9136-9148, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Daniel T. Ramotsoela, Gerhard P. Hancke, and Adnan M. Abu-Mahfouz, "Practical Challenges of Attack Detection in Microgrids Using Machine Learning," *Journal of Sensor and Actuator Networks*, vol. 12, no. 1, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Izhar Ahmed Khan et al., "An Enhanced Multi-Stage Deep Learning Framework for Detecting Malicious Activities from Autonomous Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 25469-25478, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Poojith U. Rao, Balwinder Sodhi, and Ranjana Sodhi, "Cyber Cloud Security Enhancement of Smart Grids via Machine Learning-A Review," *21st National Power Systems Conference*, Gandhinagar, India, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Reza Sepehrzad et al., “A Multi-Agent Deep Reinforcement Learning Paradigm to Improve the Robustness and Resilience of Grid Connected Electric Vehicle Charging Stations Against the Destructive Effects of Cyber-Attacks,” *Energy*, vol. 307, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ulaa AlHaddad et al., “Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks,” *Sensors*, vol. 23, no. 17, pp. 1-29, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Arastoo Zibaeirad et al., “A Comprehensive Survey on the Cloud Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities,” *Arxiv*, pp. 1-30, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Ujas Bhadani, “Pillars of Power System and Cloud Security of Smart Grid,” *International Journal of Innovative Research in Science Engineering and Technology*, vol. 13, no. 7, pp. 13888-13893, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Pengfei Yang, “Electric Vehicle Based Smart Cloud Model Cyber Cloud Security Analysis using Fuzzy Machine Learning with Blockchain Technique,” *Computers and Electrical Engineering*, vol. 115, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Neha Gupta, and Nidhi Gupta, *An Overview of E-Mobility-Based Threats to the Power Grid: Introduction to Smart Grids and Mobility Ecosystem*, E-Mobility in Electrical Energy Systems for Sustainability, pp. 1-14, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Mohsen Khalaf et al., “A Survey on Cyber-Physical Cloud Security of Active Distribution Networks in Smart Grids,” *IEEE Access*, vol. 12, pp. 29414-29444, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Meriem Aoudia et al., “Toward Better Blockchain-Enabled Energy Trading Between Electric Vehicles and Smart Grids in Internet of Things Environments: A Survey,” *Frontiers in Energy Research*, vol. 12, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] CIC EV Charger Attack Dataset 2024 (CICEVSE2024), University of New Brunswick, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/evse-dataset-2024.html

[27] R. Kalaiyarasi et al., “Enhancing Security and Confidentiality Using Trust Based Encryption (DHPKey) in Cloud Computing,” *14th International Conference on Computing Communication and Networking Technologies*, Delhi, India, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]