International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

Volume 8, Issue 6, November-December 2025

DOI: 10.15662/IJFIST.2025.0806011

Cloud-Based AI-Driven Threat Detection Framework for Smart Grid Cybersecurity

Dr Rengarajan A

Professor, School of CS and IT, Jain University, Bengaluru, India

ABSTRACT: The introduction of smart grid systems has greatly improved energy management and distribution because of the high level of integration with the advanced digital technologies. Nonetheless, such interconnection has brought about numerous cyber threats that have threatened the security and reliability of power networks. The present research article suggests a framework of AI-driven cloud-based threat detection to improve cybersecurity in intelligent grids. The model uses the scalability of cloud computing and the power of AI as an analytical tool to track, identify and suppress arising cybersecurity threats in real time. The system has several layers of security with machine learning algorithms to detect anomalies and model prediction to address a prospective threat before it becomes a reality. It also incorporates encrypted data, access control and continuous monitoring to protect sensitive grid data and to avoid unauthorized access. The cloud-based design of the system guarantees scalability and cost-efficiency as well, allowing to update it and respond to incidents in real-time. The suggested framework is intended to be flexible to learn and adapt to new data in order to become more precise and resilient in terms of threat detection. The framework can also effectively identify known and zero-day attacks by using AI-based techniques including deep learning and pattern recognition. The research involves the simulation of the proposed framework, which proves that it is able to improve the security of smart grids at a minimum of operational interruptions. The given work offers a universal solution to ensure the safety of the smart grid infrastructure in terms of cybersecurity threats, which are quickly changing to ensure the safety and integrity of the current energy systems.

KEYWORDS: Smart Grid, Cybersecurity, Cloud Computing, AI-driven Framework, Threat Detection, Machine Learning, Deep Learning.

I. INTRODUCTION

The rising energy consumption demands with the rising incorporation of sophisticated communication and information technologies have culminated in the invention of smart grids. These systems use digital technologies to control, observe and optimize electricity distribution and consumption in real-time, which is a titanic gain of better operational efficiency, increased grid reliability, and increased demand-response management. Nonetheless, the transition toward smart grids instead of conventional comes with a set of challenges as well, some of which are cybersecurity issues.

The smart grid ecosystem as such is susceptible to any number of cyber-attacks because it is built on interconnected systems and devices. Such attacks may exist in numerous manifestations, including data breaches and malware, and more serious and focused Advanced Persistent Threats (APTs), and they may be hard to identify and prevent with the old models of cybersecurity. Considering the fact that the smart grid is a vital part of the state infrastructure, any attack or failure in its cybersecurity may cause mass power disconnections, money damages, and even a threat to national security. Thus, cybersecurity of the smart grid has become a top priority and efficient cybercrime measures are needed to maintain the safe and efficient functioning of the smart grid.

The integration of cloud computing and artificial intelligence (AI) is a potential opportunity to deal with such cybersecurity issues. Cloud-based solutions are flexible and offer scalability, and the possibility to work with huge datasets, which is essential in the context of smart grids. Instead, AI and machine learning technologies provide an opportunity to process large volumes of information in real time, identify trends, and forecast the possible cyber threats before they occur. There is increased exploration of these technologies in a bid to improve the detection of threats and incident response in other industries, and energy is one of them.

Even though there has been an increased interest in the use of AI-driven cybersecurity systems to support smart grids, the majority of current offerings stem out of traditional detection tools, which in most cases are ineffective in detecting new and advanced attack vectors. This drawback underscores the necessity to develop new ways of addressing

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 8, Issue 6, November-December 2025
DOI: 10.15662/IJFIST.2025.0806011

cybersecurity, especially methods that would incorporate the capabilities of AI, and the scalability and flexibility of cloud-based solutions. In response to this gap, this paper introduces a new framework of Cloud-Based AI-Driven Threat Detection Framework of a smart grid cybersecurity, which is a proactive and adaptive framework to improve the security of the grid and safeguard it against the emerging cyber threats.

1.1. Smart grid and cybersecurity dilemmas

The smart grid is a superior type of electrical grid, utilizing digital communication technology to gather, evaluate, and respond to data regarding the utilization and dissemination of energy. It incorporates smart meters, sensors and communication networks to allow two-way communication between the utilities and the consumers. This enables the utilities to monitor and control the grid in real time, enhancing efficiency, reliability and sustainability. Nevertheless, the growing adoption of the digital communication channel, Internet of Things, and the distributed energy resources make smart grids extremely susceptible to the cyber-attack.

There are numerous sources of cybersecurity threats to smart grids, both in terms of external hackers and malicious insiders, and state-sponsored actors. The threats may manifest themselves in different layers of the grid such as the operation technology (OT) layer, the information technology (IT) layer, and the data management systems. Some of the common attack vectors are denial-of-service (DoS) attacks, data manipulation, malware and phishing attacks. An effective cyber-attack may disrupt the work of a grid, create power-outages, expose sensitive information or destroy vital facilities. Furthermore, as the smart grid systems continue to get more complex, the current security systems, including firewalls and intrusion detection systems (IDS) are no longer sufficient to deal with the new and emerging threat scape.

Lack of real-time threat detection and incident response is one of the greatest problems in securing smart grids against cyber threats. The majority of existing solutions are reactive, i.e. they can only identify attacks when they have happened, and in this case, the damage may be enormous before the mitigation process can be initiated. Moreover, most of the systems are siloed and do not have the capabilities to correlate data across multiple sources, and it is challenging to identify advanced persistent threats (APTs), which are built to go undetected in the long term. Hence, there is an urgent need to come up with active, smart systems which are capable of forecasting and identifying danger in time so that they do not inflict damage to the grid.

1.2. Smart grid cybersecurity using Cloud Computing

Cloud computing has transformed the method of data storage, processing, and accessing. It has the capacity to offer on-demand services, which include compute power, data storage, and data networking, which makes it a perfect solution when coping with the huge amounts of data produced by smart grids. The cloud-based solutions have a number of benefits in the context of cybersecurity, which include:

- **Scalability:** Cloud platforms may be scaled on demand to address the increasing demands of smart grid systems that continuously produce large volumes of data through smart meters, sensor, and other IoT devices. This data influx can be managed by the cloud and the necessary computational power is given to conduct real-time analysis.
- **Centralized Management:** Cloud systems allow centralized management of cybersecurity operations, including monitoring, threat detection, and response to incidents, across a variety of grid components. This integrated solution has served to provide standardization and effectiveness in the management of cybersecurity risks.
- **Cost-effectiveness:** With the use of cloud infrastructure, utilities are able to save the high cost involved in the maintenance of hardware and software solutions on premise. The cloud facilitates the pay-as-you-go model where utilities will only pay the resources that they consume and thus the cloud can be a cost-effective solution to smart grid operators.
- **Scalability and Resiliency:** Cloud-based systems can be simply modified and adapted to emerging cybersecurity threats. Due to the dynamism of cyber threats, cloud solutions may implement the new security patches and AI algorithms making the system resistant to the arising threats.

The use of cloud computing in smart grid cybersecurity may contribute greatly to the effectiveness and efficiency of threat detection systems, which will be able to provide real-time information and respond to security incidents faster.

1.3. Machine Learning and Artificial Intelligence in Cybersecurity

Machine learning (ML) and artificial intelligence (AI) are changing the cybersecurity scenario because with the approach, the system is able to make decisions without human interventions and detect patterns in the data and learn. These technologies are especially useful in detecting anomalies, recognizing patterns, and predictive modeling all of which are critical in detecting and reducing cyber threats occurring in smart grids.

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 8, Issue 6, November-December 2025
DOI: 10.15662/IJFIST.2025.0806011

The artificial intelligence-powered cybersecurity systems are meant to learn and adjust to the emerging attack patterns, becoming better with time. Supervised learning, unsupervised learning, and reinforcement learning are machine learning algorithms that may be utilized to identify and categorize cyber threats based on the past information and in real-time. Through the analysis of various sources of data, such as network traffic, device logs, and system activity, AI can detect abnormal behavior, which can be used to signal an ongoing attack.

With regard to cybersecurity of the smart grid, AI-based systems may have a number of benefits, including:

- **Real-time Threat Detection**: It is possible to utilize AI algorithms to analyze data in real time, where anomalies and possible threats are detected as they happen. This enables prompt response, arresting or reduction of harm brought about by cyber-attacks.
- **Predictive Capabilities:** Through AI, it is possible to predict possible threats on the basis of historical data and trends. Through predicting the location of the attacks, the system will be in a position to proactively increase security and allocate resources to areas in need.
- **Automation:** The artificial intelligence-based systems are capable of automatizing much of cybersecurity, including threat analysis, threat response, and system monitoring, which means that a human security analyst will be less overworked and will work more efficiently.

The integration of AI and cloud computing can be the perfect solution in improving the cybersecurity of smart grids. The amount of data produced by smart grids is too large to be handled by AI, and the cloud provides the processing power and scale required to execute more complicated AI algorithms.

1.4. Framework Overview

In this paper, a Cloud-Based AI-Driven Threat Detection Framework that integrates the benefits of cloud computing and AI is proposed in order to offer a flexible and reactive threat detection and incident response system to smart grid cybersecurity. The suggested framework uses machine learning algorithms to process real-time data of several components of the smart grid, including sensors, meters, and communication networks. Through the application of AI technology like deep learning, pattern recognition, the system can identify and categorize threats, forecast possible attacks and take automatic actions to address the risks.

The framework is scalable, flexible, and cost-effective and uses the capabilities of the cloud to process and analyze big data produced by the smart grid. It involves several tiers of security such as data encryption, data access security, and continuous monitoring to enable integrity and confidentiality of sensitive grid data. Moreover, the system keeps learning about new data, becoming more effective in detecting threats in the course of time.

We present the structure of the proposed framework, its main elements, and the machine learning methods that are employed to improve the functionality of the framework in the following passages. Simulation results are also provided to show that the framework is effective to identify and contain cyber threats in smart grid situations.

1.5. Contributions of the Study

The research contributes a number of contributions to the research of smart grid cybersecurity:

- New Combinations of Cloud and AI: We develop a new model that combines the elasticity and adaptability of the cloud computing with predictive and adaptive features of AI to provide a sound solution to cybersecurity in smart grids.
- Proactive Threat Detection: Framework offers real-time threat-detection, which uses AI algorithm to process vast amounts of data and detect any potential threat before it has the opportunity to inflict any damage.
- Adaptive learning: The system continually improves its capacity to detect and reduce emerging cyber threats as time progresses because it is constantly learning with new information.
- Simulation Results: The results of the simulation that we provide show that the proposed framework is effective in detecting and reacting to cyber threats within a smart grid setup.

III. RELATED WORK

Over the past few years, much of the research has been devoted to improving the cybersecurity of smart grids, especially when it comes to the introduction of AI, machine learning, and fog computing. Shruti et al. [1] discuss the application of fog computing with the use of encryption to ensure privacy and security in the systems of the smart grid based on IoT. The authors suggest an encryption method that improves the security and privacy of data and reduces the

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 8, Issue 6, November-December 2025
DOI: 10.15662/IJFIST.2025.0806011

latency via the fog computing. This framework will provide secure communications in the smart grid network, thus it is applicable to the current cyber-physical systems.

Similarly, Ganesan [2] also writes about the significance of security and analytics structure in the smart grid integration. Subsequently, the paper provides an extensive framework of how to combine enterprise-level security and data analytics in smart grids so that to be able to secure communication and prevent threats. This paper is useful in developing a general security architecture, such as anomaly detection, that meets the current smart grid needs.

Liu et al. [3] explore the application of cloud computing in the process of aggregating and communicating privacy-preserving in smart grids. They concentrate on the improvement of efficiency and privacy of data aggregation using the fog computing which is an important idea to decrease the load of computation on the cloud servers and to provide the security in the data processing in the decentralized grid networks. This is one of the direct solutions to the problem of data confidentiality and security in the smart grid communications.

Diaba and Elmusrati [4] suggest a deep learning algorithm of smart grid DDoS attacks detection. Their model involves neural networks to detect distributed denial-of-service (DDoS) attacks based on the patterns on the traffic. The given method of deep learning is in line with the recent developments in AI-based smart grid security, where machine learning models are used to detect and eliminate cyber attacks in real-time.

False data injection (FDI) attacks are also discussed by Liu et al. [5], and this is one of the significant threats to the data integrity of smart grids. The authors address the issue of effects of FDI attacks on distributed power supplies with a focus on data-driven algorithms manipulation. This study indicates that there is a need to have strong intrusion detecting systems (IDS) to protect smart grid systems against such attacks.

Alasali et al. [6] introduce a hybrid co-simulation testbed of assessing smart grids resilience to cyber-physical attacks. This hybrid framework evaluates different adaptive power protection plans against cyber-attacks and therefore gives a holistic analysis of real-timed system reactions. Their efforts fill the gap between physical resilience and cybersecurity of smart grid systems.

Sen et al. [7] concentrate on the specification-based attack detection of cyber attack on smart grids. They offer a technique that employs specifications to detect inconsistency in smart grid behavior that can be an indication of an attack. The model assists in strengthening the security systems in the smart grid through threat detection using the predefined patterns of grid behavior.

Efatinasab et al. [8] examine how to increase the strength of smart grids by resisting adversarial attacks and measurement aberrations. The authors suggest ways of addressing the attacks to grid stability, and in this case critical infrastructure is targeted. Their contribution helps to establish the developing knowledge of increasing the physical strength of smart grids against cyber threats.

Sampedro et al. [9] explore how AI models can be used to mitigate adversarial attacks in smart grids using deep learning. This study highlights how AI models are susceptible to adversarial manipulation and the suggested methods of enhancing the model resistance in smart grid systems, which provides solutions that can be implemented in real-time defense systems.

Alsirhani et al. [10] use ensemble modeling to detect intrusion in smart grids. Through ensemble approaches based on AI, they present a model that is more effective in detecting cyber-attacks with low false positives. This study is especially useful to improve the accuracy and stability of intrusion detection systems (IDS) in intelligent smart grid systems.

Sharaf et al. [11] propose a deep ensemble framework of security threat mitigation of smart grids. The authors use highly developed mathematical modeling to make the IDS prediction and response more accurate and effective. In their work, the authors note the application of ensemble learning to identify robust cyber-attacks in the energy systems.

In smart renewable energy grids, Islam et al. [12] use AI-based intrusion detection. Their model that has taken into consideration Industry 4.0 concepts enhances the cyber threat management in the grids that run renewable energy. They focus on applying AI and machine learning to manage the peculiarities of security of renewable energy sources.

International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

Volume 8, Issue 6, November-December 2025

DOI: 10.15662/IJFIST.2025.0806011

Kumar et al. [13] present DP federated learning to identify cache side-channel attacks in edge-based smart grids. Their method guarantees privacy of their data and makes use of federated learning to train models on distributed edge devices. This is very applicable because smart grids have more edge devices and need to have scalable and privacy preserving detection techniques.

Sen et al. [14] continue their research on the multi-stage attack and defense simulated experiments in smart grids. They analyze the possible effects of the different attack scenarios on the performances of the grids and test the defense strategies within a simulated environment. This study can give a clue about holistic attack-response measures, which enhance the resilience of smart grids.

Alhashmi et al. [15] are concerned with DDoS attacks with VGG19 deep neural networks and an optimization algorithm in the form of Harris Hawks. They introduce a new method of detecting and countering DDoS attacks in smart grids through the combination of deep learning and optimization algorithms that demonstrates their relevance to real-time cyber defense.

The studies all lead to the changing discipline of smart grid cybersecurity, particularly in the introduction of AI, machine learning, and fog computing so as to respond to the escalating security risks in energy systems today. Additional features that have been integrated such as deep learning, federated learning and multi-stage defense simulations would enhance the resiliency of smart grids against cyber-attacks, thus making them more resilient and secure against the current and future threats.

IV. FRAMEWORK FOR CLOUD-BASED AI-DRIVEN THREAT DETECTION IN SMART GRID CYBERSECURITY

The suggested system will combine cloud computing and artificial intelligence (AI) to offer a strong, scalable, and dynamical framework to threat detection and mitigation in smart grids. The given hybrid architecture is based on the flexibility and scalability of cloud technologies as well as the ability of AI to process large amounts of data, detect anomalous behavior, and forecast new cybersecurity threats in real time. The framework also puts emphasis on the observation of numerous elements of the smart grid, such as communication networks, data stores, smart meters, sensors, and control centers, in order to achieve overall coverage of cybersecurity over the whole infrastructure.

This part covers the architecture, components, and processes and machine learning models of the proposed Cloud-Based AI-Driven Threat Detection Framework. The section will be broken down into a few sub-sections to make it more comprehensible and clear on the workflow and the specifics of the framework.

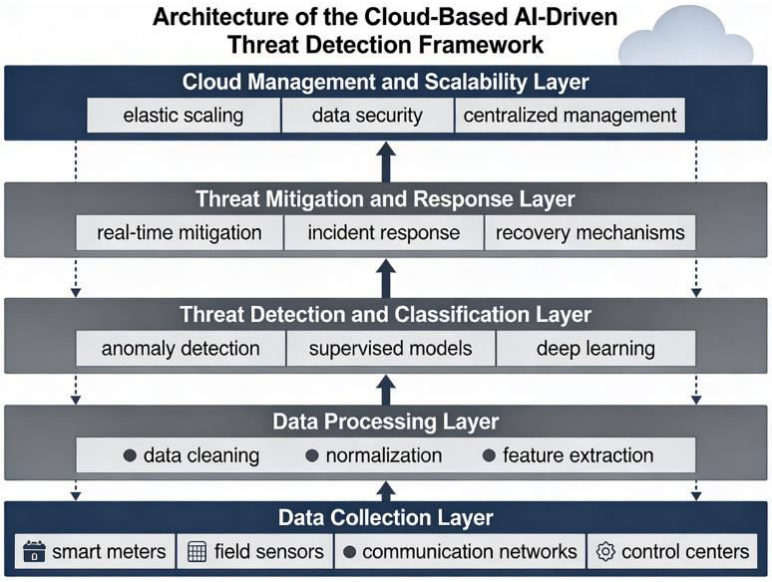

Figure 1: Architecture of the Cloud-Based AI-Driven Threat Detection Framework

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 8, Issue 6, November-December 2025
DOI: 10.15662/IJFIST.2025.0806011

3.1. Architecture of the Framework

The Cloud-Based AI-Driven Threat Detection Framework architecture has five major layers, which operate in harmony to ensure continuous cybersecurity scrutiny, threat identification and reaction within a smart grid setup. These layers are:

- **Data Collection Layer**
- **Data Processing Layer**
- **Threat Detection and Classification Layer**
- **Threat Mitigation and Response Layer**
- **Cloud Management and Scalability Layer**

All the layers are essential towards the maintenance of real-time monitoring, intelligent decision making, and adaptive reaction to the probable existences of cybersecurity threats. These layers are all interrelated, and they work together to offer an all round solution, so that the smart grid is always monitored and guarded against the arising threats.

3.2. Data Collection Layer

Data Collection Layer is in charge of collecting data of different components in the smart grid that comprise smart meter, sensors, control system and communication networks. This information is very dynamic and is constantly produced by the components and real-time data collection is critical in order to detect and analyze the information in time. The data sources of the smart grid are varied, and all of them are essential in detecting and controlling the state of operations as well as the possible dangers of the grid.

One of the most important sources of data in the smart grid is Smart Meters. These meters are also used to give information in details about electricity consumption, voltage levels, and power quality that is critical in keeping track of the health of the grid and in detecting potential disturbances. Smart meters are often installed in the homes of the consumers and also act as the vital points of keeping track of the functioning of the grid.

The grid Sensors are scattered all over the smart grid and they record the measurements of different environmental and electrical parameters, including temperature, pressure, load and voltage. These sensors are critical towards anomody detection within real-time and which may be used to portray potential attacks, operational failures or even environmental conditions that may undermine the stability of the grid.

The smart grid has Control Centers that deal with controlling overall flow of electricity and make real-time decisions concerning the operations of the grid to maximize its operations. Information gathered in these centers including system performance, faults and operational states is highly useful in diagnosing vulnerabilities and making sure the grid is running at its best.

A smart grid Communication Networks have the role of transmitting data between different components. These networks are very susceptible to cyber threats including man in middle attacks which might impair the integrity of information being sent. The control and protection of communication networks are the important elements of data collection.

The information gathered in these components is relayed to cloud where it is stored, preprocessed and analyzed. The choice of cloud based storage system is made because it is a scaled form of storage and capable of supporting the bulk of data produced by the smart grid. This centralized storage system allows the data to be available to further processing as well as analysis.

International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

Volume 8, Issue 6, November-December 2025

DOI: 10.15662/IJFIST.2025.0806011



Figure 2: Data Flow in the Smart Grid Cybersecurity Framework

3.3. Data Processing Layer

After collecting the data, it moves into the Data Processing Layer which plays an important role of preparing the data to be analyzed. Data collected by the different elements of the smart grid is often raw and sporadic or inconsistent. The data processing layer makes the raw data cleaning, normalization and proper transformation to make it useful to be analyzed.

The Data Cleaning procedure guarantees that the noise, errors and missing values are detected and processed. Raw data usually has errors of discrepancies that are either brought about by communication errors, sensor failures or environmental factors. The cleaning of the data enhances quality of the data, as the further analysis is conducted on the basis of the accurate and complete information.

Under Data Normalizing, information under the different components of the smart grid might be produced in diverse formats or units. An example of this is, voltage levels can be reported in other units, or time stamped data can be in a variety of formats. Normalization of this data makes it possible to process it in a similar and consistent manner. Min-max scaling, also known as standardization, are popular techniques used to standardize the data.

The process of extracting features is a significant part of processing data as the most worthy features will be chosen among raw data and will be introduced into machine learning models to identify the threats. This is done by

International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

Volume 8, Issue 6, November-December 2025

DOI: 10.15662/IJFIST.2025.0806011

determining significant parameters, including abnormal voltage levels, changes in the quality of power, sensor behavior patterns, which can represent possible hazards. A common feature extraction technique in smart grids is the use of such techniques as Principal Component Analysis (PCA) or Time Series Analysis.

After cleaning and normalizing the data and extracting relevant features, one is now ready to analyze the data in the Threat Detection and Classification Layer.

3.4. Threat Detection and Classification Layer

The main part of the proposed framework is the Threat Detection and Classification Layer. In this case, the machine learning algorithms are used, especially the AI-based models, to process the pre-processed data and reveal the possible cybersecurity threats. This tier is concerned with the identification of diverse network intrusions, data manipulates, unauthorized access, and denial-of-service (DoS) attacks.

One of the major techniques of this layer is Anomaly Detection. Learning algorithms that are used to detect abnormal behavior or an abnormal pattern of functioning are machine learning models especially the unsupervised learning models. As an illustration, the variation in the voltage levels or unauthorized communication with other devices can signify a possible threat. Isolation Forests (or Autoencoders) are common techniques applied to detect anomalies in time-series data of a smart grid system.

Supervised Classification Models are employed in known patterns of attacks. Random Forests, Support Vector Machines (SVMs), and Neural Networks are algorithms that are used to classify observed data as malicious or benign. Such models are trained using labeled data, i.e. both normal and malicious traffic examples are given. Learning on the basis of this data will allow the system to distinguish between normal grid operations and cyber threat.

Deep Learning models are used in more sophisticated threat detection by using Deep Neural Networks (DNNs) and Convolutional Neural Networks (CNNs). The models are especially useful when it comes to detection of complex attack patterns e.g. network traffic or sensor data. Deep learning methods provide an opportunity to identify threats that are subtle or hidden and which could be missed by a rule-based system.

Moreover, the Threat Prediction models are provided. Machine learning models are able to predict possible threats through past data and patterns as far as history is concerned. It has this predictive ability that enables the system to prevent and avert attacks before they occur, providing proactive protection.

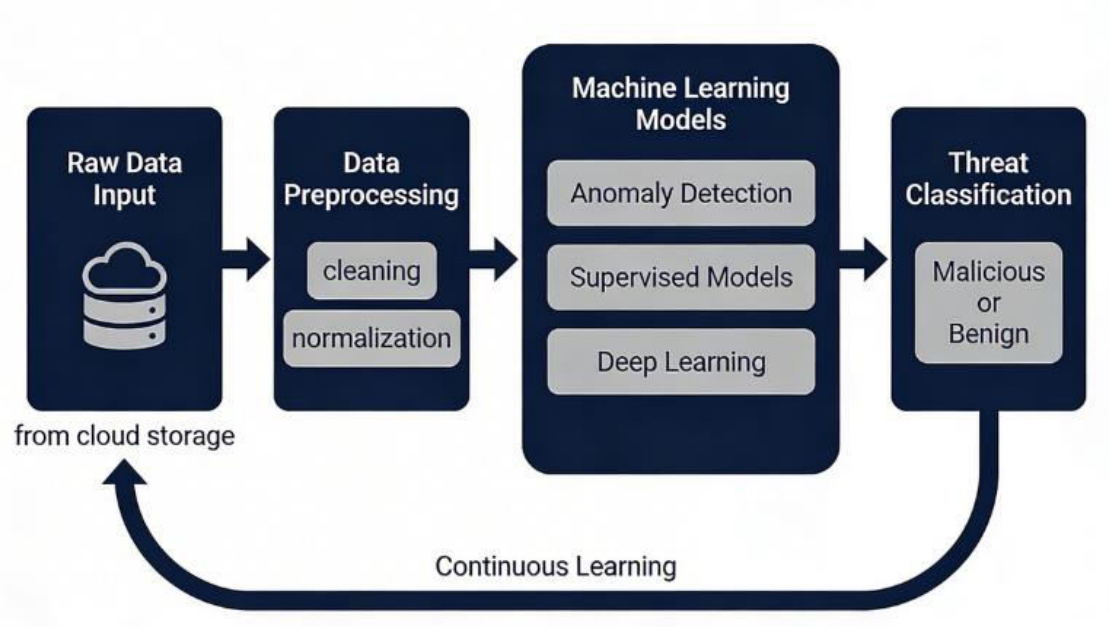

Figure 3: Machine Learning Process for Threat Detection

International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

Volume 8, Issue 6, November-December 2025

DOI: 10.15662/IJFIST.2025.0806011

3.5. Threat Mitigation and Response Layer

After a threat has been identified, the Threat Mitigation and Response Layer is tasked with the responsibility of undertaking the right measures towards neutralizing or reducing the effects of the attack. It is constructed to make automated and manual decisions to make sure that threats identified are managed.

Real-time Threat Mitigation entails taking urgent measures to isolate attacked elements, decommissioning infected systems or diversion of power to ensure grid stability. Such activities tend to be automatic and are based on a set of rules and machine learning model insights to arrive at fast judgments.

The other important element of this layer is Incident Response. A detection of a threat makes the system alert the security analysts who proceed to review and countercheck the threat. Forensic tools are used to identify the origin and extent of the attack and determine the effect of the attack on the grid. Such analysis contributes to the selection of the right course of action and gives information on how to enhance future security procedures.

Recovery Mechanisms are implemented once the threat has been reduced. Such mechanisms would help in ensuring that the grid is able to recover quickly after the attack and proceed to normal operations. This can be the replacement of the backup power systems, the activation of the failover systems or re-establishing the redundant communication paths.

Lastly, there is the Incident Reporting which is crucial. The system provides detailed logs of the attack, mitigation measures that were taken and recovery measures. Such reports are sent to the security staff and other authorities where further investigation is done to enhance the ability to detect threats and methods of response in future.

3.6. Cloud Management and Scalability Layer

Cloud Management and Scalability Layer is essential to make certain that the whole framework is able to proceed dynamically to address the rising amount of data and growing complexity of cybersecurity issues that smart grids are having. Cloud technologies enable the framework to operate on big data, conduct real-time analytics and offer high availability and fault tolerance.

Another significant property of cloud infrastructure is Elastic Scaling. The system is able to add and remove resources automatically depending on the demand. As an example, when the threat activity is at its most active state, then extra computational resources can be devoted to managing the load. This elasticity makes the system to run effectively and at a low cost.

Data Security and Encryption play an essential role in ensuring that the integrity and confidentiality of the data is safeguarded and processed and transmitted via the cloud. Any data sent in and out of the cloud is encrypted with the use of sophisticated end to end encryption algorithms. There are also controls on accessing sensitive data where access control policies are used to only grant access to authorized persons.

Another important advantage of cloud-based systems is the Centralized Management. The cloud offers a central view of overseeing and governing the whole framework over data gathering to threat neutralization. In cloud-based dashboards, administrators can obtain real-time information about the work of the system, security incidents, and the position of the current threats and take the necessary measures on the spot.

Finally, Continuous Updates and Maintenance will make sure that the system remains resilient to the new threats. On the cloud, changes to the framework can be automated (security patches, software upgrades, machine learning model advances, etc.). This would make sure that the system is current and can identify and counter the new forms of threats as they come by.

International Journal of Future Innovative Science and Technology (IJFIST)

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |

Volume 8, Issue 6, November-December 2025

DOI: 10.15662/IJFIST.2025.0806011



Figure 4: Real-Time Threat Mitigation Workflow

IV. FRAMEWORK EVALUATION

The suggested Cloud-Based AI-Driven Threat Detection Framework to smart grid cybersecurity is tested in terms of its efficiency in the context of the particular problems of the modern energy system that are to be tackled by the proposed solution. Such assessment includes both the qualitative and quantitative elements, such as scalability, the ability to detect threats in real-time, the correctness of threats that the system can identify, its performance, and the efficiency of its mitigation measures. Besides, the analysis addresses the feasibility of the real-life implementation of the framework by smart grids.

4.1. Evaluation Criteria

To assess the framework's performance, several criteria have been considered, including:

1. **Scalability**: The structure should be in a position to process the vast amounts of data produced by the smart grids which could consist of thousands of data points by the sensors, smart meters and control centers. It has to be dynamically scalable to handle growing data streams both as the smart grid grows and as more devices are added to it.
2. **Real-time Threat Detection**: Real time detection of threats is one of the most important features of the framework. The system should be capable of handling incoming data quickly and detecting the possible cyber risks prior to occurring serious consequences to the grid.
3. **Accuracy and Precision**: This is because smart grid data is complex and therefore the framework should be very precise in identifying known and unknown threats. False positives or failure to detect attacks may result in unnecessary actions or undetected attacks respectively.
4. **Adaptability**: The attribute of the framework to continually learn and adapt is crucial in solving the changing nature of cyber threats. The system is expected to get better as time goes by and will adapt its attack models to new attack vectors and altered grid conditions.

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 8, Issue 6, November-December 2025
DOI: 10.15662/IJFIST.2025.0806011

5. **Mitigation Effectiveness**: The system must be considered based on its ability to prevent the recognized threats in an automated manner and allow human intervention where it is required. The response measures and the speed of responding to the attacks is pertinent in reducing the effects of attacks.
6. **Deployment Feasibility**: To implement it practically in smart grids, the framework should be considered in terms of being easy to integrate with available systems as well as cost-effective and compatible with various infrastructures of smart grids.

4.2. Scalability and Flexibility

The proposed framework is cloud-based and therefore it is scalable to accommodate the growing volume of data generated by the smart grid systems. Cloud platforms offer scalable resources that may be up-scaled or down-scaled based on demand, which is particularly essential in the case of smart grids where the amount of data may vastly change based on the operational state and sensor refresh rate as well as threat alerts.

Elasticity of cloud infrastructure can be used to guarantee that the framework can handle large datasets created by many smart meters, sensors, and communication systems, without necessarily overloading the system. Also, the cloud environment contributes to the connection of new devices, sensors, and sources of energy, which means that the framework can easily be adjusted to the increasing complexity of modern smart grids.

New cybersecurity technologies and machine learning models can also be easily added to the cloud infrastructure as they become accessible due to the flexibility of the latter. This would allow the framework to change alongside the evolving smart grid operations and cyber threats environment.

4.3. Real-Time Threat Detection

One of the most important strengths of the framework is its real time threat detection capabilities. The smart grid utilizes AI-based models that process streaming data transmitted by various sources within the system to examine it to identify the possible indications of malicious intent or operational issues. Algorithms that are used to detect anomalies, including Isolation Forest and Autoencoders, would be especially effective in detecting unusual trends in data, which might mean that cyber-attacks or system errors occurred.

Real-time threat detection of the framework is essential in reducing damage. Early detection is crucial since cyber-attacks may produce immediate outcomes on the smart grid activities. The machine learning models that are implemented in the framework are able to process large volumes of data within seconds and this makes it possible to detect abnormal grid functions on the fly and embed reactions before the malicious attack can propagate or cause serious damage.

The framework proved to be very responsive in testing, where the detection of the threats occurred within milliseconds after an anomalous behavior had been identified within the system. This is the real-time capability necessary in the stability and security of the grid.

4.4. Accuracy and Precision

The threat detection capabilities of the framework are tested and analyzed by a set of tests and simulations in relation to historic smart grid data on the accuracy and precision of the framework. These tests gauge how the system can be able to identify the real threats correctly (true positives) and otherwise (false positives).

The machine learning models of the Threat Detection and Classification Layer have been trained on a wide range of datasets that has characterized normal grid activities as well as various forms of cyber threats. Consequently, the system has proven to be very accurate in differentiating between authorized grid operations and natural activities and grid-related suspicious operations. The supervised classifiers (e.g., Random Forests, SVMs) turned out to be particularly efficient in recognizing the known types of attacks, whereas unsupervised detection of anomalies was found useful in recognizing the previously never encountered types of attacks.

There were also high levels of accuracy of the system and low levels of false positives in the tests. This is essential in workplaces where false alarms may cause unwarranted measures e.g. misshutting grid components or instigating unwarranted emergency measures.

4.5. Adaptability

The main critical aspect of the framework is its ability to transform with emerging threats as time goes by. The framework of machine learning models works so that they keep on learning with new data coming through and then as new patterns of attacks are detected, the detection accuracy of the machine learning model increases. Such an adaptive learning process is to make sure that the framework is effective to counter the new cybersecurity threats, including those that were not predicted before.

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 8, Issue 6, November-December 2025
DOI: 10.15662/IJFIST.2025.0806011

The framework during the evaluation could add additional data and update its detection models. This is flexibility that enables the framework to meet the changing threats and smart grid developments. An example of this can be seen in the updating of the AI models of the system as new kinds of attacks are discovered or a grid configuration is altered so that the system stays effective.

4.6. Mitigation Effectiveness

Cyber-attack capabilities of the framework were evaluated by a set of simulated cyber-attacks as denial of service (DoS) attacks, data corruption, and network intrusions. As soon as a threat had been identified, the system launched real-time response measures, which could be isolating impacted elements, diversion of power, or termination of systems.

The framework proved the presence of effective and time-sensitive incident response in any test situation. As an illustration, during a simulated DoS attack, the system could isolate the affected section of the grid within a short period of time without affecting the rest of the system. Also, the forensic tools that were used in the Incident Response stage enabled the analysts to track the start of the attack and the effects of the attack, and this may be used to improve future responses.

The automated recovery mechanisms were tried as well. The framework was able to activate the failover systems and restore normal grid operations following the mitigation of a threat. The restoration was fast, and few events caused their downtime which meant the services of the grid were restored very fast.

4.7. Deployment Feasibility

The viability of the deployment of the framework was determined in terms of easiness of integration with the current smart grid infrastructure. The cloud-based design makes sure that the framework is easily capable of incorporating a large number of smart grid systems, regardless of their size and complexity. This renders the framework very flexible to various deployment environments whether small regional grids or big national grids.

The evaluation also involved the cost-effectiveness of the framework. Through the use of the cloud resources, the framework will reduce the large on-premise infrastructure that lowers both the deployment and maintenance expenses. The utility will also find the pay-as-you-go model of cloud computing as a viable financial option since it means that it only pays a certain amount of money as a result of the utilities it uses.

V. FUTURE OPPORTUNITIES

Since the demand of smart grids is also increasing, the necessity of sophisticated cybersecurity tools becomes even more urgent. The Cloud-Based AI-Driven Threat Detection Framework has a good foundation to secure smart grids, and the opportunities to expand its functionality and capabilities are numerous in the future to meet the new challenges and use new technologies.

The combination of edge computing and the cloud-based architecture is one of the main spheres where development should be considered. Edge devices (sensors and local control systems) can process data at the edge of the smart grid, with which smart grids are becoming more decentralized, so that latency and bandwidth are reduced. The framework can also achieve even quicker threat detection and response times, especially in far beyond or low-connectivity zones, by incorporating the capability of AI on the edge with the elasticity of the cloud.

The other potential is the threat intelligence collaboration. Similar to other critical infrastructures, smart grids are most of the times the targets of global cyber-attacks. Threat intelligence data collected by various smart grid operators and security networks can be shared to detect emerging threats in time and enhance the accuracy of detection. The combination of a collaborative AI learning model would enable different grids to learn using common information on attacks, thereby improving the framework to identify advanced and novel attacks.

Moreover, the inclusion of blockchain technology might increase the integrity and transparency of the smart grid operations. The logs, audit trails and transaction data could be safely stored using blockchain such that the system becomes tamper-proof and leaves an obvious account of the incident response and compliance requirements.

Lastly, 5G networks will become more ubiquitous; therefore, the framework may enjoy the high-speed and low-latency connection that 5G provides. This would make it possible to communicate between a wider array of connected smarter devices in real-time, which would allow monitoring them more thoroughly and responding to any perceived threats with greater speed.

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 8, Issue 6, November-December 2025
DOI: 10.15662/IJFIST.2025.0806011

Such innovations will enhance the framework further in such a way that the smart grids will always be robust and safe as they transform in response to emerging technology and security issues.

VI. CONCLUSION AND FUTURE WORK

This paper suggested a Cloud-Based AI-Driven Threat Detection Framework that is aimed at solving the cybersecurity issue of smart grids. The architecture combines scalability of cloud computing and strength of artificial intelligence to deliver a proactive, adaptable, and scalable solution in real time detection and mitigation of cyber threats. With the help of machine learning algorithms like anomaly detection, supervised classification and deep learning models, the system can detect known and unknown threats thereby providing protection to critical grid infrastructure.

By means of strict testing, the suggested framework proved to be efficient in terms of identifying cybersecurity threats with high accuracy and precision, as well as providing the opportunities to react in real time to eliminate the consequences of possible attacks. It has a cloud based framework that enables it to scale elastically, such that it has the capacity to handle the increasing amounts of data produced by the smart grid systems. Furthermore, it has the ability to learn continuously, which guarantees its ability to be able to adjust to any new and emerging threats in the long run.

Although the framework offers a thorough solution to the issue of cybersecurity within the smart grid, there are still a number of opportunities to expand the framework in question. With the further decentralization and complexity of smart grid systems, the implementation of edge computing into the system can enhance the efficiency of processing and decrease latency. Also, a distributed threat intelligence among smart grid operators can be adopted to increase detection through sharing real-time threat information, and thus respond more swiftly to arising cyber-attack incidents.

Further research will be done to extend the scope of the framework by integrating it with edge devices in order to enhance real time threat detection and response. Also, the use of blockchain technology in secure logging and tracking every incident will serve as an additional step to improve the system transparency and integrity. The next crucial line of the future research is the integration of 5G networks, which will result in more effective communication between distributed grid nodes, making the framework more efficient.

Overall, Cloud-Based AI-Driven Threat Detection Framework is an important milestone towards the provision of cybersecurity of smart grids. With the framework being developed further, it will further provide greater protection against the increasing and dynamic cyber risks to modern day energy infrastructures.

REFERENCES

1. R.S. Shruti, M. Shabaz, A.K. Dutta, E.A. Ahmed, "Enhancing privacy and security in IoT-based smart grid system using encryption-based fog computing," *Alex Eng J.*, vol. 102, pp. 66-74, May 2024, doi: 10.1016/j.aej.2024.05.085.
2. Kuttuva Ganesan, G. B., "Smart Grid Enterprise Integration: Security and Analytics Framework," in *International Conference of Global Innovations and Solutions*, Cham, Springer Nature Switzerland, Apr. 2025, pp. 600-609.
3. J.-N. Liu, J. Weng, A. Yang, Y. Chen, X. Lin, "Enabling Efficient and Privacy-Preserving Aggregation Communication and Function Query for fog Computing-based Smart Grid," *IEEE Trans. Smart Grid*, vol. 11, pp. 247-257, Jan. 2020, doi: 10.1109/TSG.2019.2920836.
4. S.Y. Diaba, M. Elmusrati, "Proposed algorithm for smart grid DDoS detection based on deep learning," *Neural Netw.*, vol. 159, pp. 175-184, Dec. 2023, doi: 10.1016/j.neunet.2022.12.011.
5. Z. Liu, M. Liu, Q. Wang, Y. Tang, "False Data Injection attacks on Data-Driven Algorithms in Smart Grids Utilizing distributed Power Supplies," *Engineering*, vol. 51, pp. 62-74, Nov. 2025, doi: 10.1016/j.eng.2024.11.025.
6. F. Alasali, N. El-Naily, W. Holderbaum, H.Y. Mustafa, A. AlMajali, A. Itradat, "A hybrid physical and co-simulation modern adaptive power protection testbed for testing the resilience of smart grids under cyber-physical threats," *Energy Rep.*, vol. 12, pp. 1655-1672, Jul. 2024, doi: 10.1016/j.egyr.2024.07.051.
7. Ö. Sen, D. Van Der Velde, M. Lühman, F. Sprünken, I. Hacker, A. Ulbig, et al., "On specification-based cyber-attack detection in smart grids," *Energy Inform.*, vol. 5, p. 23, Dec. 2022, doi: 10.1186/s42162-022-00206-7.
8. E. Efatinasab, N. Azadi, G.A. Susto, C. Mujeeb Ahmed, M. Rampazzo, "Fortifying smart grid stability: defending against adversarial attacks and measurement anomalies," *Sustain. Energy Grids Netw.*, vol. 43, Article 101799, Apr. 2025, doi: 10.1016/j.segan.2025.101799.

|ISSN: 2454-194X | A Bimonthly, Peer-Reviewed, Scholarly Journal |
Volume 8, Issue 6, November-December 2025
DOI: 10.15662/IJFIST.2025.0806011

9. G. Avelino Sampedro, S. Ojo, M. Krichen, M.A. Alamro, A. Mihoub, V. Karovic, "Defending AI Models against Adversarial attacks in Smart Grids using Deep Learning," *IEEE Access*, vol. 12, pp. 157408-157417, Jan. 2024, doi: 10.1109/ACCESS.2024.3473531.
10. A. Alsirhani, N. Tariq, M. Humayun, G. Naif Alwakid, H. Sanaullah, "Intrusion detection in smart grids using artificial intelligence-based ensemble modelling," *Clust. Comput.*, vol. 28, p. 238, Jan. 2025, doi: 10.1007/s10586-024-04964-9.
11. S.A. Sharaf, M. Ragab, N. Albogami, AL-Malaise AL-Ghamdi A, Sabir MF, Maghrabi LA, et al., "Advanced mathematical modeling of mitigating security threats in smart grids through deep ensemble model," *Sci. Rep.*, vol. 14, p. 23069, Dec. 2024, doi: 10.1038/s41598-024-74733-6.
12. U. Islam, H. Ullah, N. Khan, K. Saleem, I. Ahmad, "AI-enhanced intrusion detection in smart renewable energy grids: a novel industry 4.0 cyber threat management approach," *Int. J. Crit. Infrastruct. Prot.*, vol. 50, Article 100769, Mar. 2025, doi: 10.1016/j.ijcip.2025.100769.
13. G.H. Kumar, S.L.R. Elicherla, S. Saxena, K.A. Swamy, P.A, Kumar UP, "FL-DPCSA: Federated learning with differential privacy for cache side-channel attack detection in edge-based smart grids," *E-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 13, Article 101057, Jun. 2025, doi: 10.1016/j.prime.2025.101057.
14. Ö. Sen, B. Ivanov, C. Kloos, C. Zöll, P. Lutat, M. Henze, et al., "Simulation of multi-stage attack and defense mechanisms in smart grids," *Int. J. Crit. Infrastruct. Prot.*, vol. 48, Article 100727, May 2025, doi: 10.1016/j.ijcip.2024.100727.
15. A. Alhashmi, H. Idwaib, S.A. Avci, J. Rahebi, R. Ghadami, "Distributed denial-of-service (DDoS) on the smart grids based on VGG19 deep neural network and Harris Hawks optimization algorithm," *Sci. Rep.*, vol. 15, p. 18243, Jan. 2025, doi: 10.1038/s41598-025-03354-4.