Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

AN INTELLIGENT MULTI-LAYERED MACHINE LEARNING AND BIG DATA ANALYTICS FRAMEWORK FOR AUTONOMOUS CYBER THREAT DETECTION, ADAPTIVE DEFENSE MECHANISMS, AND SECURE CLOUD-NATIVE SMART ELECTRICAL POWER GRID CYBER-PHYSICAL INFRASTRUCTURE

Kaleem Ullah[*1], Azaan Athar[2], Omer Naveed[3], Abdullah Zubair[4], Usama Ahmad Mughal[5]

[*1]*Department of Computer Science, Bacha Khan University, Charsadda, Pakistan*
[2]*Department of Science and Engineering, Macquarie University, Sydney, Australia*
[3]*Plant Manager, Oursun Pakistan Ltd, 50MWp Solar Power Generation Power Plant, Senior Member ISA USA, Member IEEE USA and PMI USA.*
[4]*Department of Software Engineering, Virtual University of Pakistan, Pakistan*
[5]*Department of Cyber Security, NASTP Institute of Information Technology Lahore, Pakistan*

[*1]kaleem2668@gmail.com, [2]azaan.athar@students.mq.edu.au, [3]onaveed@yahoo.com, [4]abdullah69zubair@gmail.com, [4]bc220420516azu@vu.edu.pk, [5]usamaahmad@niit.edu.pk

DOI: https://doi.org/10.5281/zenodo.19692765

Keywords
Smart grid cybersecurity, Cyber-physical systems, Machine learning, Big data analytics, Autonomous threat detection, Adaptive defense, Cloud-native security, Critical infrastructure protection.

Article History
Received: 31 January 2026
Accepted: 16 March 2026
Published: 30 March 2026

Corresponding Author: *
Kaleem Ullah

Abstract

The rapid digitalization of smart electrical power grids has significantly improved operational efficiency, automation, and real-time decision-making. However, it has also increased the exposure of cyber-physical infrastructure to sophisticated and evolving cyber threats. As modern smart grids increasingly rely on cloud-native architectures, distributed sensors, intelligent control systems, and interconnected communication networks, traditional rule-based and static cybersecurity mechanisms are no longer sufficient to ensure resilient and adaptive protection. This paper proposes an intelligent multi-layered framework that integrates machine learning and big data analytics for autonomous cyber threat detection, adaptive defense mechanisms, and secure cloud-native management of smart electrical power grid cyber-physical infrastructure. The proposed framework is designed to address the growing complexity, scale, and heterogeneity of cyber threats targeting critical energy systems. The framework consists of multiple coordinated layers, including data acquisition, preprocessing, feature engineering, anomaly detection, threat classification, adaptive response, and secure cloud orchestration. At the core of the proposed architecture, machine learning models are employed to identify malicious activities, abnormal communication patterns, false data injection attacks, denial-of-service incidents, insider threats, and other advanced persistent threats affecting the cyber-physical components of the grid. Big data analytics techniques are incorporated to process high-volume, high-velocity, and high-variety operational data generated from smart meters, supervisory control and data acquisition systems, phasor measurement units, IoT devices, and distributed energy management platforms. This enables the framework to support real-time situational awareness, predictive threat intelligence, and continuous risk assessment. In addition, adaptive defense mechanisms are embedded within the framework to enable dynamic mitigation,

automated policy updates, attack containment, and resilience enhancement under changing threat conditions. The cloud-native design further improves scalability, interoperability, and deployment flexibility while supporting secure resource management across distributed grid environments. The proposed framework aims not only to detect cyber threats with high accuracy but also to enhance response speed, reduce false alarms, and improve the overall security posture of critical smart grid infrastructure. This research contributes to the development of next-generation intelligent cybersecurity solutions for energy systems by combining autonomous learning, data-driven threat analytics, and resilient cloud-native defense strategies. The study offers a practical and scalable pathway toward securing future smart grid cyber-physical ecosystems against increasingly complex cyber attacks while supporting reliability, sustainability, and operational continuity in critical power networks.

1- Introduction:

The electrical power sector is currently experiencing a profound transformation driven by digitalization, decentralization, automation, and the growing integration of intelligent communication technologies. Traditional power grids, which were once largely centralized and mechanically controlled, are being replaced by smart electrical power grids that combine physical energy infrastructure with digital monitoring, communication, and control capabilities. This new generation of power systems integrates smart meters, supervisory control and data acquisition (SCADA) systems, phasor measurement units (PMUs), Internet of Things (IoT) devices, distributed energy resources, cloud platforms, and real-time analytics tools to improve operational efficiency, grid stability, fault management, and energy optimization. As a result, smart grids have become a key foundation for modern energy sustainability, renewable integration, demand-side management, and intelligent utility operations [1]. Despite these advantages, the convergence of cyber and physical components has also created serious cybersecurity concerns. Unlike conventional electrical systems, smart grid environments rely on continuous data exchange, remote connectivity, software-defined services, edge-to-cloud communication, and automated control loops. These features significantly increase the vulnerability of the grid to cyberattacks. Adversaries may exploit communication protocols, cloud services, endpoint devices, and control platforms to launch attacks that compromise data integrity, confidentiality, and operational availability. Cyber intrusions in smart grids can lead to power outages, control disruption, equipment damage, false command execution, load instability, market manipulation, and even cascading infrastructure failures [2]. Because electrical grids are part of national critical infrastructure, such attacks may also result in broad economic losses, public safety risks, and reduced trust in digital energy systems. The cybersecurity challenge becomes even more severe in cloud-native smart grid environments. Cloud-native architectures offer scalability, elasticity, service modularity, and efficient resource orchestration for modern grid applications. However, containerized workloads, virtualized services, application programming interfaces, distributed microservices, and hybrid cloud-edge deployments introduce additional threat vectors that traditional security solutions are not designed to manage effectively. Signature-based intrusion detection systems and static firewall-based protection mechanisms often fail to identify zero-day attacks, intelligent malware, false data injection, insider threats, and advanced persistent threats operating across multiple cyber-physical layers [3]. Furthermore, the large volume, velocity, and variety of data generated in smart grid ecosystems make manual monitoring and static analysis increasingly impractical. To address these limitations, intelligent and adaptive cybersecurity solutions have become essential. Machine learning

techniques provide the ability to learn hidden attack patterns, detect anomalous behavior, classify known and unknown threats, and continuously improve detection accuracy using historical and real-time data. In parallel, big data analytics enables large-scale processing, correlation, filtering, and interpretation of diverse grid data streams collected from operational technologies and information technologies. When combined, machine learning and big data analytics can support autonomous cyber threat detection, predictive security analysis, and real-time defense decision-making in complex smart grid ecosystems. These capabilities are especially important in cyber-physical environments where rapid threat detection and coordinated response are critical to maintaining operational continuity. The proposed research is motivated by the need for a unified, multi-layered, and cloud-compatible security framework capable of protecting smart electrical power grid cyber-physical infrastructure against dynamic and intelligent cyber threats [4]. Rather than relying on isolated detection modules or fragmented security policies, the study introduces a comprehensive framework that integrates data acquisition, preprocessing, feature engineering, anomaly detection, threat classification, adaptive defense, and secure cloud-native orchestration into a coherent architecture. Such a framework can improve situational awareness, reduce false alarms, accelerate response actions, and enhance resilience under changing attack conditions. The significance of this research lies in its interdisciplinary integration of cybersecurity, machine learning, big data analytics, and smart grid engineering. It recognizes that future power systems cannot be protected by conventional cybersecurity models alone. Instead, resilient smart grids require intelligent and data-driven defense mechanisms that can operate autonomously across distributed, heterogeneous, and cloud-enabled infrastructures. The proposed framework therefore seeks not only to detect cyber threats with high precision but also to enable adaptive mitigation strategies that preserve system reliability, service availability, and infrastructure trustworthiness. In practical terms, the framework is intended to support multiple smart grid applications, including substation monitoring, SCADA protection, intelligent meter security, network traffic analysis, distributed energy resource coordination, and cloud-hosted energy management services [5]. By enabling continuous monitoring and autonomous threat response, the framework can help utility operators and decision-makers strengthen the security posture of critical energy systems while supporting digital transformation objectives. This makes the study highly relevant for modern power utilities, cybersecurity researchers, energy regulators, and infrastructure planners seeking scalable and future-ready grid protection strategies. Table 1 summarizes the major cybersecurity challenges in smart electrical power grid cyber-physical infrastructure and highlights the role of intelligent machine learning and big data-driven solutions in addressing them.

Table 1: Key cybersecurity challenges in smart grid cyber-physical infrastructure and intelligent mitigation perspective.

Smart grid challenge	Description	Security impact	Role of machine learning and big data analytics
Large-scale data generation	Smart grids produce massive real-time data from sensors, meters, PMUs, and control devices	Makes manual analysis difficult and delays threat recognition	Enables automated data processing, pattern extraction, and threat correlation
Heterogeneous infrastructure	Integration of IT, OT, IoT, cloud, and edge devices creates diverse operational environments	Expands attack surface and complicates unified protection	Supports cross-domain analysis and intelligent classification of abnormal events

Advanced cyber threats	Includes false data injection, ransomware, denial-of-service, malware, and insider attacks	Threatens grid reliability, confidentiality, and operational safety	Detects hidden attack signatures and anomalous system behavior
Dynamic attack evolution	Attack techniques continuously adapt and bypass static defenses	Reduces effectiveness of rule-based and signature-based systems	Learns evolving patterns and improves detection over time
Cloud-native vulnerabilities	Microservices, APIs, containers, and distributed cloud services introduce new weaknesses	Increases exposure to remote exploitation and service disruption	Provides scalable analytics and real-time cloud security monitoring
Real-time response requirements	Power systems require immediate reaction to security incidents	Delayed response can trigger outages and cascading failures	Enables fast threat prediction, prioritization, and adaptive defense actions

In light of these concerns, this paper proposes an intelligent multi-layered machine learning and big data analytics framework for autonomous cyber threat detection, adaptive defense mechanisms, and secure cloud-native smart electrical power grid cyber-physical infrastructure. The framework is designed to unify intelligent analytics with real-time defense coordination in order to protect critical smart grid assets against increasingly sophisticated cyber threats. Through this approach, the research aims to contribute to the development of secure, resilient, and scalable smart grid ecosystems capable of supporting the future of digital energy infrastructure.

2- Smart Grid Cyber-Physical Infrastructure and Emerging Security Concerns:

The transformation of conventional electrical power systems into smart grid cyber-physical infrastructure has significantly changed the generation, transmission, distribution, and management of electricity. Unlike traditional grids, smart grids integrate physical power equipment with digital communication systems, intelligent sensors, automated controllers, cloud platforms, and advanced monitoring technologies. This integration improves operational efficiency, fault detection, renewable energy coordination, demand-response capability, and real-time decision-making. Through this cyber-physical convergence, utility operators can monitor grid behavior more accurately and respond to dynamic changes with greater speed and precision. However, the same interconnectivity that strengthens grid intelligence also creates major cybersecurity challenges [6]. Because smart grids depend on continuous communication between physical devices and digital platforms, vulnerabilities in the cyber layer can directly affect physical grid operations. A cyberattack on a control center, communication network, smart meter, or SCADA platform may lead to data corruption, false operational commands, equipment malfunction, service disruption, or instability in grid performance. This close coupling between cyber and physical domains makes smart grid systems more exposed and more sensitive to malicious interference than conventional power networks. Researchers have shown that smart grid cyber-physical infrastructure is vulnerable to a wide range of threats, including false data injection attacks, denial-of-service attacks, spoofing, malware infiltration, ransomware, insider threats, and advanced persistent threats. These attacks may target critical components such as SCADA systems, phasor measurement units, smart meters, communication gateways, cloud services, and distributed control units. In contrast to traditional information systems, cyberattacks in smart grids can produce immediate physical consequences such as frequency disturbances, relay failure, voltage

instability, transformer stress, and localized or regional outages. This makes cybersecurity a fundamental requirement for maintaining the safety, reliability, and resilience of modern energy infrastructure [7]. Another important concern is the growing use of cloud-enabled and distributed digital platforms in smart grid environments. Cloud-native technologies improve scalability, storage, and analytics performance, but they also introduce additional risks related to remote access, API vulnerabilities, workload compromise, and data leakage. As a result, traditional rule-based and signature-based security mechanisms are no longer sufficient to protect increasingly dynamic and data-intensive smart grid ecosystems. The literature therefore emphasizes the need for intelligent, adaptive, and multi-layered protection mechanisms capable of detecting and responding to evolving cyber threats in real time. Table 2 presents the main smart grid components, their operational roles, and associated security concerns.

Table 2: Major smart grid components and associated cybersecurity concerns

Component	Role in smart grid	Key security concern	Possible impact
SCADA systems	Supervisory monitoring and operational control	Unauthorized access and malware	Loss of visibility and control disruption
PMUs	Real-time synchronized measurement	False data injection and spoofing	Inaccurate state estimation
Smart meters	Consumption monitoring and communication	Data tampering and privacy breach	Billing errors and demand-response disruption
Communication networks	Data exchange across grid layers	Denial-of-service and interception	Delayed or blocked control signals
Cloud platforms	Data storage, analytics, and service hosting	API exploitation and data leakage	Service interruption and reduced security

Figure 1 presents a conceptual overview of the smart grid cyber-physical architecture by illustrating the interaction between physical power system components, digital communication networks, intelligent monitoring devices, and cloud-enabled control platforms. It also highlights the major categories of cybersecurity threats affecting this interconnected infrastructure, including false data injection, denial-of-service attacks, malware infiltration, spoofing, insider threats, and other malicious activities that may disrupt grid stability, compromise data integrity, and reduce operational reliability.

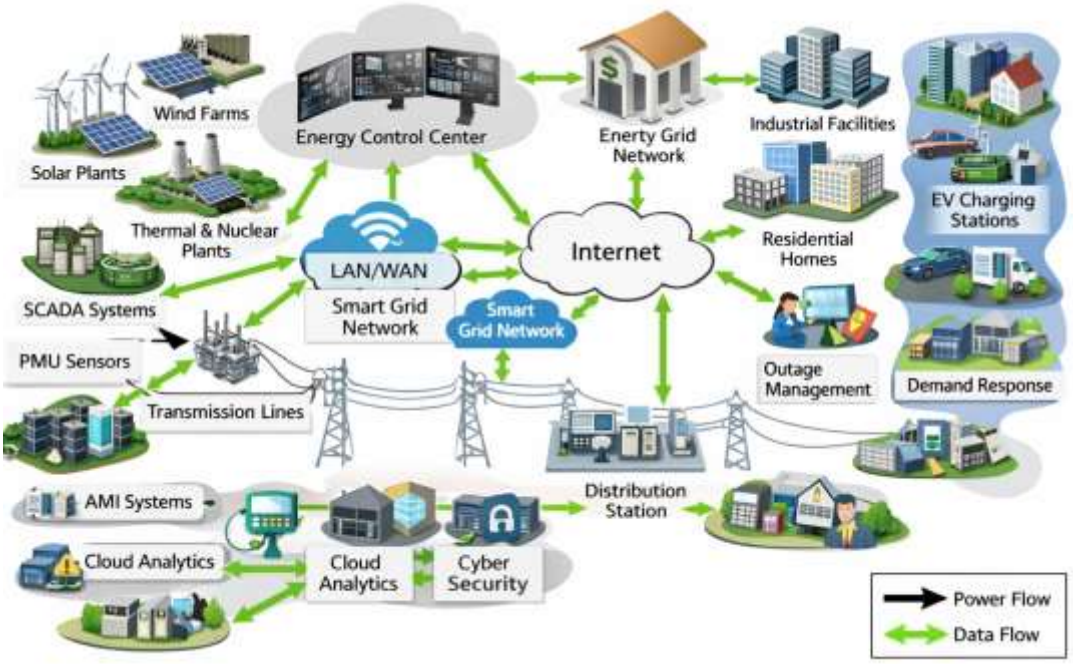

Figure 1: Conceptual overview of smart grid cyber-physical infrastructure and emerging security concerns.

The literature recognizes smart grid cybersecurity as a critical research area because the increasing digitalization of power infrastructure has created both new capabilities and new risks. Protecting smart grid cyber-physical systems now requires advanced and intelligent security frameworks that can preserve operational continuity while defending against sophisticated and evolving cyber threats.

3- Adaptive Defense Mechanisms and Autonomous Response Strategies:

Beyond cyber threat detection, recent cybersecurity research increasingly emphasizes the importance of adaptive defense mechanisms that can respond intelligently and dynamically to changing attack conditions. In highly interconnected and time-sensitive environments such as smart grid cyber-physical infrastructure, identifying an attack is only the first step; the system must also be capable of taking appropriate defensive action before the threat escalates into a larger operational disruption. For this reason, adaptive defense has become a central concept in the design of modern security architectures for critical infrastructure. In the context of smart grids, adaptive defense refers to the ability of the system to monitor threat conditions continuously, interpret attack severity, and modify its security behavior in real time with minimal human intervention. This may include updating security policies, isolating compromised devices, reconfiguring communication routes, blocking malicious traffic, restricting unauthorized access, prioritizing alerts, redistributing computational resources, and initiating mitigation procedures to preserve operational continuity. Unlike static defense mechanisms, adaptive strategies are designed to evolve according to system behavior, threat intelligence, and environmental conditions [8]. This makes them more suitable for protecting dynamic infrastructures where attack methods are increasingly sophisticated, distributed, and difficult to predict in advance. The literature shows that multiple adaptive defense approaches have been explored in recent years. Some studies rely on expert rule-based systems, where predefined security logic is used to trigger defensive actions after attack detection. Other works employ game-theoretic models to analyze attacker–defender interactions and identify optimal response strategies under uncertainty. Software-defined networking (SDN) has also received significant attention because it enables

centralized and programmable control over network behavior, allowing suspicious traffic flows to be redirected, filtered, or blocked dynamically. In addition, moving target defense strategies aim to reduce attacker success by continuously changing system configurations, network paths, or resource locations. More advanced studies have investigated reinforcement learning-based defense models, in which the system learns effective response strategies through continuous interaction with the threat environment [9]. Self-healing architectures have also emerged as promising solutions, allowing compromised nodes or services to be automatically repaired, restored, or replaced to maintain resilience. A major strength of adaptive defense is its potential to reduce response delay in critical infrastructure systems. In smart grids, time is a crucial factor because cyber incidents can quickly propagate from digital components into physical power system operations. A delayed response to a malicious command, abnormal measurement pattern, or compromised communication channel may lead to voltage instability, relay malfunction, transformer overload, service interruption, or even cascading outages across wider grid regions. Therefore, the literature consistently identifies autonomous and real-time defensive capability as a key requirement for smart grid security. Detection without rapid mitigation is often insufficient in environments where the cost of inaction can be extremely high. At the same time, existing research reveals several limitations. Many adaptive defense models are designed for specific attack types only, such as denial-of-service mitigation, false data injection response, or network rerouting under communication attacks. While these approaches can be effective within narrow contexts, they often lack generalizability across heterogeneous smart grid environments. Some studies present strong attack detection performance but offer little support for autonomous mitigation, meaning that alerts still depend on manual interpretation by operators. Other models implement automated response actions but are not supported by sufficiently intelligent threat analysis, which may lead to inappropriate or inefficient defensive behavior. In some cases, frameworks remain simulation-specific and do not fully consider the complex interactions among grid devices, communication networks, cloud platforms, and operational priorities. Another limitation highlighted in the literature is the fragmented treatment of defense layers. Detection, analysis, decision-making, and response are often studied as separate modules rather than as part of a coordinated and closed-loop security framework [10]. This separation reduces the effectiveness of autonomous defense because response decisions depend heavily on accurate threat interpretation, contextual understanding, and system-wide visibility. For example, isolating a suspicious node may improve security but also affect service reliability if operational dependencies are not considered. Similarly, blocking communication traffic may stop an intrusion attempt but may also interfere with legitimate control actions if the defense logic lacks situational awareness. These challenges demonstrate that adaptive defense in smart grids must balance cybersecurity requirements with power system stability, operational continuity, and resilience objectives. For this reason, the literature increasingly points toward the need for integrated frameworks in which threat detection, security analytics, adaptive decision-making, and response execution operate in coordination. Such frameworks should be able to evaluate attack severity, identify affected infrastructure layers, estimate operational consequences, and select the most suitable mitigation strategy in real time. They should also support feedback loops so that the outcomes of defensive actions can improve future detection and response accuracy. In smart grid cyber-physical systems, this coordinated approach is especially important because the environment is distributed, data-intensive, and dependent on both cyber and physical state awareness. Table 3 summarizes the major adaptive defense approaches reported in the literature and their relevance to smart grid cybersecurity.

Table 3: Adaptive defense approaches and their relevance to smart grid cybersecurity

Adaptive defense approach	Core principle	Application in smart grids	Key limitation
Rule-based automated response	Uses predefined security rules to trigger actions	Alert generation, access restriction, basic attack containment	Limited flexibility against new or unknown threats
Game-theoretic defense	Models attacker–defender interaction for optimal response	Strategic response planning under adversarial uncertainty	May be computationally complex for real-time deployment
Software-defined networking (SDN) defense	Dynamically manages traffic flows and network policies	Traffic filtering, rerouting, communication isolation	Depends on secure and reliable central control
Moving target defense	Continuously changes system configuration to reduce attack predictability	Dynamic network path switching and service relocation	Implementation complexity in large-scale infrastructures
Reinforcement learning-based defense	Learns optimal response actions from interaction with the environment	Adaptive mitigation, policy optimization, intelligent defense selection	Requires training stability and quality reward design
Self-healing architecture	Automatically restores or replaces compromised components	Service recovery, fault tolerance, resilience improvement	May require significant infrastructure support

Figure 2 presents a conceptual view of adaptive defense and autonomous response within a smart grid cyber-physical environment by illustrating how threat detection, security analytics, decision-making, and mitigation actions are interconnected across multiple operational layers. It highlights the flow from attack identification to intelligent response execution, including actions such as alert prioritization, node isolation, traffic filtering, communication rerouting, policy adjustment, and system recovery, while also emphasizing the feedback mechanisms that enable the framework to continuously adapt to evolving cyber threats and maintain grid stability, resilience, and operational continuity.

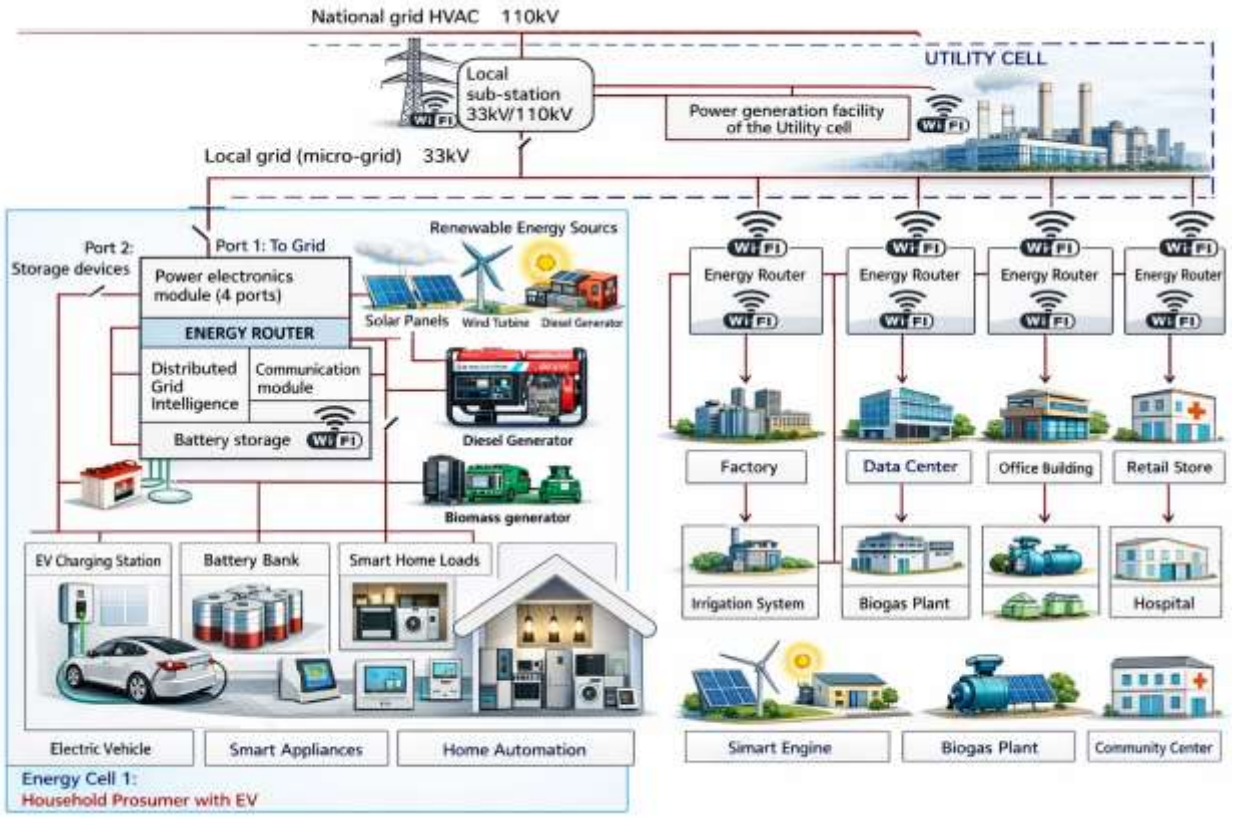

Figure 2: Adaptive defense and autonomous response strategies in smart grid cyber-physical infrastructure.

Adaptive defense has become an essential requirement in modern smart grid cybersecurity because static and isolated security mechanisms are no longer sufficient to protect critical infrastructure against evolving and multi-stage attacks. The literature makes it clear that future smart grid protection must go beyond passive monitoring and incorporate autonomous response capabilities that are intelligent, coordinated, and operationally aware. This understanding supports the development of integrated multi-layered security frameworks in which detection, analytics, and adaptive defense function together to maintain both cybersecurity and power system resilience.

4- Methodology:

This study adopts a systematic, design-oriented, and simulation-based methodology to develop an intelligent multi-layered framework for autonomous cyber threat detection, adaptive defense mechanisms, and secure cloud-native smart electrical power grid cyber-physical infrastructure. The methodology is structured to examine how machine learning, big data analytics, and adaptive cybersecurity strategies can be integrated into a unified architecture for protecting modern smart grid systems against dynamic and sophisticated cyber threats [11]. It includes the modeling of smart grid cyber-physical environments, multi-source data acquisition, preprocessing and feature extraction, intelligent threat detection, adaptive response design, cloud-native security integration, and performance evaluation. Through this approach, the study aims to ensure that the proposed framework is not only theoretically grounded but also operationally relevant, scalable, and effective for real-time cybersecurity management in critical energy infrastructure.

4.1- Research Design and Methodological Approach:

This study adopts a design-oriented, analytical, and simulation-based research methodology to develop and evaluate an intelligent multi-layered machine learning and big data analytics framework for autonomous cyber threat detection, adaptive defense mechanisms, and secure cloud-native smart electrical power grid cyber-physical infrastructure. The research design is motivated by the increasing complexity of cyber threats facing modern smart grids, where conventional static security approaches are no longer sufficient to ensure resilient and adaptive protection. Because smart grid environments are highly interconnected, data-intensive, and operationally sensitive, the study requires a methodological structure capable of integrating intelligent detection, large-scale analytics, adaptive decision-making, and distributed security orchestration into a unified framework. The design-oriented nature of the study reflects its primary objective, which is not only to analyze cybersecurity challenges but also to construct a practical and logically organized framework that can address those challenges in a systematic way. Rather than examining isolated algorithms or individual defensive tools, the research focuses on designing a coordinated multi-layered architecture in which threat detection, data processing, risk interpretation, and response execution operate as interconnected components [12]. This makes the methodological approach suitable for smart grid cyber-physical systems, where vulnerabilities often emerge from the interaction between physical infrastructure, digital communication layers, and cloud-enabled control environments. The design-oriented perspective therefore supports the development of a holistic solution rather than a single-point technical intervention. The study is also analytical in nature because it investigates the relationships among smart grid vulnerabilities, cyber threat patterns, data characteristics, intelligent detection models, and defense requirements. The analytical component of the methodology is used to identify how cyber threats propagate across different layers of the smart grid, how large-scale heterogeneous data can reveal attack behavior, and how machine learning and big data analytics can be employed to improve threat identification and response capability. This part of the methodological design helps establish the theoretical foundation of the proposed framework and ensures that the selected security layers are aligned with the operational realities of smart electrical power systems. In addition, the study is simulation-based because the proposed framework is intended to be evaluated in controlled yet realistic smart grid cyber-physical scenarios. Simulation is particularly appropriate in this domain because direct experimentation on live electrical infrastructure is often impractical, costly, and risky. By using simulated environments, the research can model different cyberattack conditions, communication behaviors, device interactions, and cloud service operations without endangering actual power system assets [13]. This enables the framework to be tested under both normal and adversarial operating conditions, allowing the study to assess not only cyber threat detection accuracy but also response efficiency, adaptability, resilience, and operational feasibility. The methodological structure is organized in a layered and sequential manner to ensure that each component of the framework is systematically designed, integrated, and assessed. The process begins with problem analysis and smart grid cyber-physical system modeling, where the major infrastructure components, cyber dependencies, threat vectors, and operational requirements are defined. This is followed by multi-source data acquisition, in which relevant data are gathered from simulated grid environments, network traffic, control system logs, sensor streams, and other security-related sources. The next stage focuses on data preprocessing and normalization to improve data quality and consistency, followed by feature engineering and attribute extraction to identify the most informative indicators of malicious or abnormal behavior. After the feature preparation stage, the methodology proceeds to machine learning-based cyber threat detection, where intelligent models are trained or configured to identify anomalies, classify known threats, and support predictive cybersecurity analysis. To

handle the scale and complexity of smart grid data, the research also includes a big data analytics layer that supports distributed data processing, event correlation, and real-time situational awareness. This analytical intelligence is then connected to an adaptive defense and autonomous response layer, which is responsible for selecting and initiating suitable mitigation strategies based on the detected threat context. Finally, the methodology incorporates cloud-native security orchestration, acknowledging the growing role of distributed cloud and edge platforms in modern smart grid environments. The complete framework is then subjected to simulation, validation, and comparative performance evaluation**.** Figure 3 illustrates the overall methodological flow of the study from conceptual problem identification to framework validation and performance analysis.

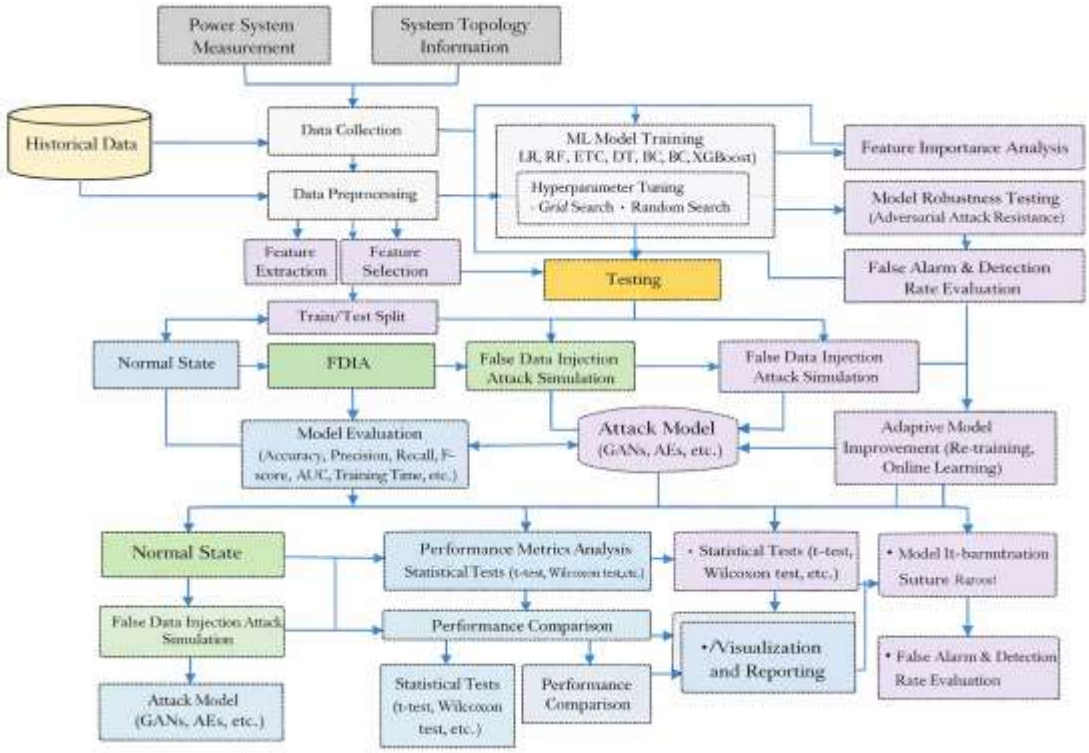

Figure 3: Overall research design and methodological flow for the proposed smart grid cybersecurity framework.

The research design and methodological approach adopted in this study provide a comprehensive foundation for developing an intelligent, scalable, and resilient cybersecurity framework for smart electrical power grid cyber-physical infrastructure. By combining design-oriented thinking, analytical rigor, and simulation-based evaluation, the methodology ensures that the proposed framework is capable of addressing both the technical complexity and the operational demands of modern smart grid cybersecurity. This structured approach also supports the broader research objective of advancing autonomous threat detection, adaptive defense, and secure cloud-native management for next-generation energy systems.

4.2- Smart Grid Cyber-Physical System Modeling:

The first stage of the proposed methodology focuses on modeling the smart electrical power grid as a cyber-physical system (CPS) composed of tightly interconnected physical power infrastructure and digital communication,

monitoring, and control components. This modeling stage is fundamental because modern smart grids no longer operate as purely electrical networks; instead, they function as intelligent and data-driven infrastructures in which physical processes and cyber operations continuously interact. The behavior of the overall system depends not only on the electrical performance of generation, transmission, and distribution assets but also on the reliability, integrity, and security of data exchange across control platforms, sensors, communication links, and cloud-enabled services. In the proposed model, the physical layer includes the major operational components of the electrical grid, such as generation units, substations, transmission lines, distribution feeders, transformers, relays, load centers, distributed energy resources, and consumer-side smart energy devices. These components are responsible for energy production, delivery, regulation, and protection. They represent the operational backbone of the smart grid and are directly associated with power quality, voltage stability, frequency control, load balancing, and service continuity. In conventional grid analysis, these assets are often examined primarily from the standpoint of electrical performance [14]. However, in a cyber-physical smart grid, their behavior is increasingly influenced by digital commands, measurement feedback, and automated control decisions. The cyber layer of the model includes SCADA systems, phasor measurement units (PMUs), smart meters, intelligent electronic devices, IoT sensors, communication gateways, data concentrators, control applications, cloud-hosted services, databases, and network management platforms. These cyber elements provide the intelligence, communication, and automation capabilities required for real-time operation of the smart grid. They collect system measurements, transmit control signals, monitor asset conditions, coordinate distributed resources, and support analytics-driven decision-making. Their role is crucial in enabling advanced grid functions such as demand response, fault detection, remote monitoring, energy forecasting, renewable energy integration, and automated network control. At the same time, their presence increases system dependency on digital connectivity and software reliability. This integrated cyber-physical modeling approach is essential because cyber threats in smart grids rarely remain confined to the digital domain. A malicious action that begins in the cyber layer, such as manipulated measurements, unauthorized control commands, or denial of communication service, can propagate rapidly into the physical layer and alter the behavior of grid assets. For example, false data injection may distort state estimation and lead to improper operational decisions; denial-of-service attacks may delay or prevent protective actions; malware may compromise control applications and affect switching or load coordination; and insider manipulation may alter system settings in ways that destabilize grid performance. Therefore, modeling the smart grid as a unified cyber-physical environment is necessary for understanding how attack scenarios translate into operational risk. Another important aspect of the modeling stage is the representation of inter-layer dependencies. In smart grids, the physical layer depends on cyber services for measurement, monitoring, and control, while the cyber layer depends on physical infrastructure for context, timing, and operational relevance. This mutual dependence means that even small anomalies in one layer may influence the performance of the other. A compromised sensor can affect state awareness, a disrupted communication channel can delay control responses, and an incorrect cloud-based analytics output can trigger suboptimal physical actions [15]. By explicitly modeling these dependencies, the study creates a stronger foundation for detecting abnormal behavior and designing intelligent defensive strategies that consider both cyber and physical consequences. The smart grid cyber-physical system model also supports the later stages of the methodology, particularly data acquisition, feature extraction, machine learning-based threat detection, and adaptive defense strategy formulation. Because the model defines the entities, communication pathways, data types, and attack points in the system, it serves as the structural basis for identifying which data should be monitored, which features may indicate

abnormal behavior, and which infrastructure components are most vulnerable to cyber disruption. In this sense, the modeling stage is not merely descriptive; it plays a direct role in shaping the design and evaluation of the proposed intelligent cybersecurity framework. From a methodological perspective, the modeling approach used in this study is designed to be both comprehensive and scalable. It is comprehensive because it includes multiple classes of physical and cyber assets, along with their interactions, dependencies, and threat exposure. It is scalable because it can be extended to different smart grid configurations, including utility-scale systems, microgrids, distributed energy networks, and cloud-assisted smart energy platforms. This flexibility is important because the proposed framework is intended to remain relevant across a range of deployment environments rather than being limited to a single simulation case. Table 4 shows the primary layers and components included in the smart grid cyber-physical system model.

Table 4: Major layers and components in the smart grid cyber-physical system model

System layer	Main components	Functional role	Security relevance
Physical power layer	Generation units, substations, transformers, relays, transmission and distribution lines, load centers	Energy generation, transmission, delivery, protection, and operational control	Directly affected by cyber-induced disruptions and control manipulation
Monitoring and sensing layer	PMUs, smart meters, IoT sensors, intelligent electronic devices	Real-time measurement, condition monitoring, event sensing, local automation	Vulnerable to spoofing, false data injection, and tampering
Communication layer	Communication gateways, routers, wired/wireless links, field networks, protocols	Data exchange between field devices, control centers, and cloud services	Exposed to denial-of-service, interception, replay, and routing attacks
Control and application layer	SCADA systems, energy management systems, control applications, operator interfaces	Supervisory monitoring, automated control, command execution, operational decision support	Targeted by malware, unauthorized access, and command manipulation
Cloud and data services layer	Cloud-hosted platforms, databases, analytics engines, storage services	Scalable computation, data analytics, remote access, orchestration, and reporting	Vulnerable to API misuse, data leakage, access compromise, and workload attacks

Figure 4 illustrates the conceptual modeling structure of the smart grid as an integrated cyber-physical system by showing the interconnection between physical power infrastructure, sensing and monitoring devices, communication networks, control platforms, and cloud-based services. It highlights how these layers operate together to support real-time data exchange, automated control, and intelligent decision-making, while also demonstrating how vulnerabilities or malicious activities within the cyber domain can propagate across the system and influence the stability, reliability, and security of physical grid operations.

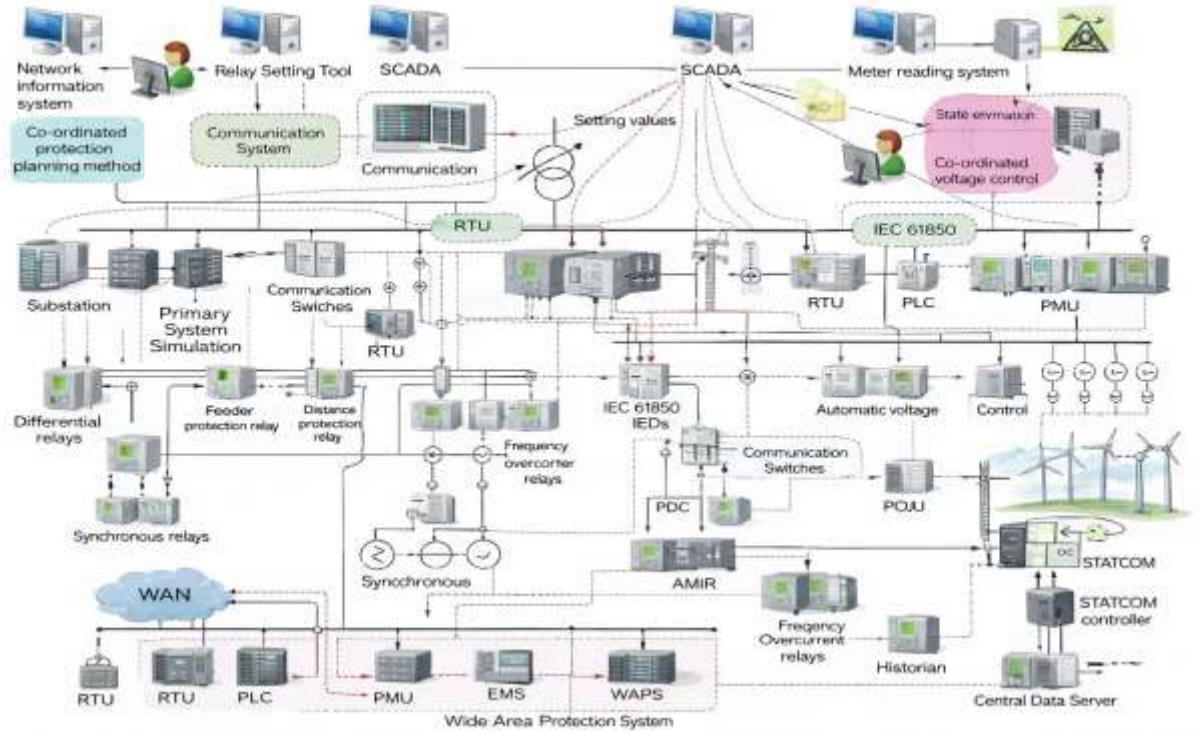

Figure 4: Smart grid cyber-physical system modeling structure for the proposed intelligent cybersecurity framework.

Smart grid cyber-physical system modeling forms the foundation of the proposed methodology by providing a structured representation of the infrastructure, data flows, operational dependencies, and attack surfaces present in modern power networks. By treating the smart grid as an integrated cyber-physical environment rather than a collection of isolated components, the study creates a realistic basis for intelligent threat detection, adaptive defense planning, and secure cloud-native cybersecurity management. This modeling stage therefore serves as a critical step in developing a framework capable of protecting modern smart electrical power systems against evolving and multi-layered cyber threats.

4.3- Data Acquisition and Multi-Source Data Collection:

The proposed methodology relies on the collection and integration of multi-source smart grid data to support machine learning and big data analytics. This stage is essential because the accuracy, robustness, and generalization ability of the proposed intelligent framework depend heavily on the quality and diversity of the acquired data. In smart grid cyber-physical environments, security-relevant information is generated by multiple interconnected sources rather than a single monitoring point. Therefore, the methodology adopts a broad data acquisition strategy to capture both normal operational behavior and abnormal conditions associated with cyber threats. The collected data may be obtained from simulated smart grid environments, publicly available intrusion detection datasets, network traffic traces, SCADA communication logs, PMU measurement streams, smart meter records, IoT device telemetry, event logs, and cloud service audit trails. The use of diverse data sources is intended to ensure that the framework reflects the real operational complexity of smart electrical power grids. Each source contributes a different view of system behavior [16]. For instance, SCADA logs provide information related to control actions and supervisory communication, PMU streams offer synchronized electrical

measurements, smart meter records reflect consumer-side activity, and cloud audit trails capture remote service interactions and access behavior. By combining these heterogeneous sources, the framework gains a more complete understanding of the cyber-physical state of the grid and becomes better equipped to identify attack patterns that may not be visible within isolated datasets. Data acquisition is designed to represent realistic smart grid conditions in which information is generated continuously and in multiple formats. These datasets may contain structured, semi-structured, or unstructured data depending on their origin and application context. Some streams, such as PMU measurements and IoT telemetry, may arrive at high speed and require near real-time collection, while others, such as event logs and audit records, may be recorded periodically or in batches. This heterogeneous data environment is important because smart grid cybersecurity depends on correlating information across physical devices, communication layers, and digital services [17]. The methodology therefore emphasizes comprehensive data coverage so that the proposed framework can learn from both steady-state system behavior and rapidly evolving threat conditions. Another important purpose of this stage is to include representative cyberattack scenarios relevant to smart grid operations. Attack-related data are categorized according to different threat types, including intrusion attempts, abnormal communication patterns, false data injection, service disruption events, anomalous sensor readings, malware propagation, unauthorized configuration changes, and insider manipulation. This makes the data environment more suitable for training, testing, and validating intelligent threat detection models. It also supports later analytical stages by ensuring that the acquired dataset contains sufficient variation to distinguish legitimate operational changes from actual cyber incidents. The data acquisition layer further supports cross-domain and cross-layer analysis. In a smart grid cyber-physical system, a single attack may influence several system layers simultaneously [18]. For example, a false data injection attack may affect sensor measurements, communication records, and control decisions at the same time, while a denial-of-service event may appear in both network traffic behavior and delayed system response logs. A multi-source data collection strategy is therefore necessary for building a framework that can identify coordinated and multi-stage threats with greater reliability. The major data sources, their functional roles, and their security relevance are present in Table 5.

Table 5: Major data sources used in smart grid multi-source data acquisition

Data source	Type of information collected	Security relevance	Example use in framework
Simulated smart grid environments	Operational scenarios, attack events, device interactions	Provides controlled and labeled smart grid behavior	Training and testing under realistic cyber-physical conditions
Intrusion detection datasets	Known attack patterns and traffic features	Supports classification of cyber threats	Benchmarking and supervised learning
Network traffic traces	Packet flows, communication behavior, connection patterns	Reveals denial-of-service, intrusion, or abnormal communication activity	Network anomaly detection
SCADA communication logs	Control commands, status messages, event records	Indicates command tampering, unauthorized access, and operational anomalies	Control-layer threat analysis

PMU measurement streams	Synchronized voltage, current, frequency, and phase data	Helps identify false data injection and abnormal grid states	Detection of measurement manipulation
Smart meter records	Energy usage, communication activity, consumer-side events	Useful for identifying tampering and abnormal device behavior	Demand-side anomaly detection
IoT telemetry and cloud audit trails	Device status, access logs, service interactions	Exposes remote access abuse, malware activity, and service misuse	Cloud-native security monitoring

Figure 5 present the conceptual structure of the multi-source data acquisition process by showing how heterogeneous smart grid data streams are gathered from different operational and cyber domains and integrated into a unified analytical pipeline. It highlights the connection between raw data collection and the subsequent stages of preprocessing, feature engineering, and intelligent threat detection within the proposed framework.

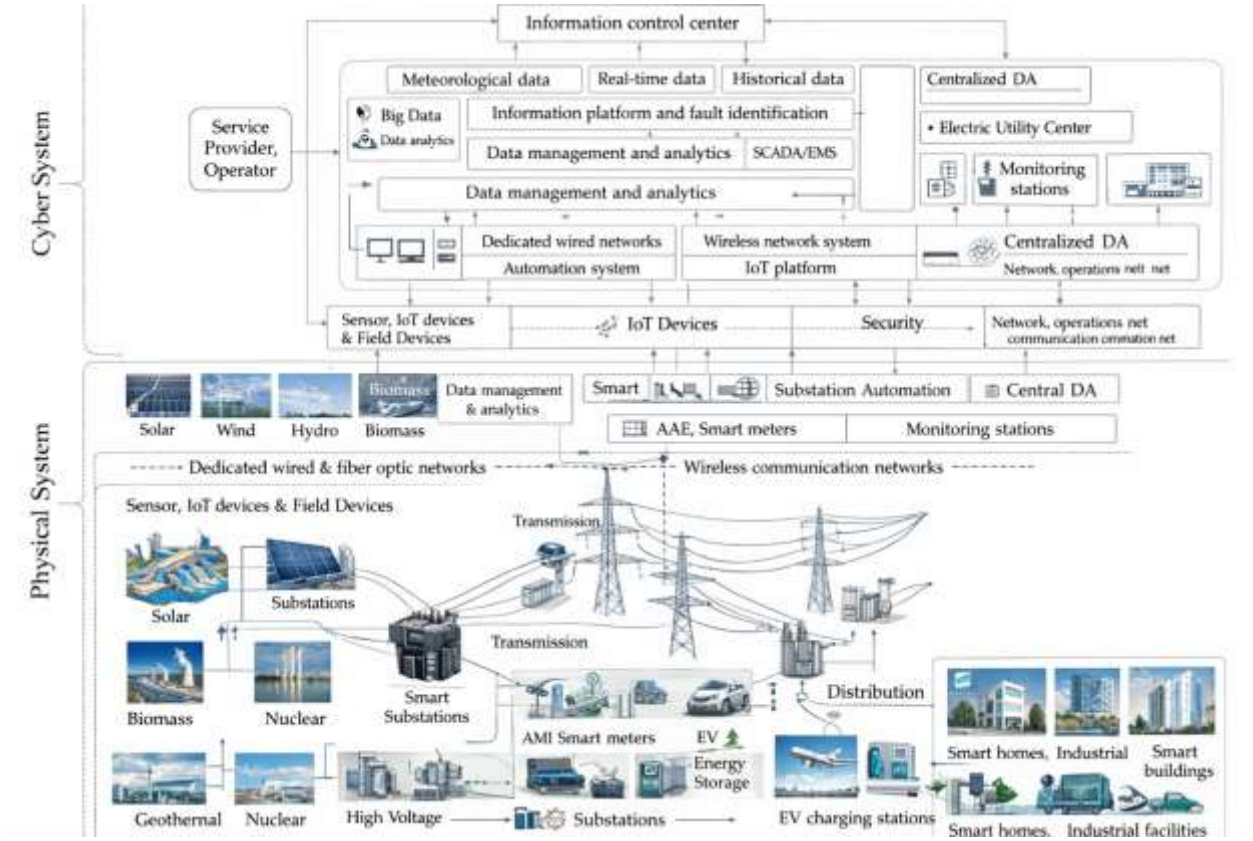

Figure 5: Multi-source data acquisition framework for smart grid cybersecurity analysis.

Data acquisition and multi-source data collection provide the foundational information layer for the proposed methodology. By gathering diverse, representative, and security-relevant data from across the smart grid cyber-physical ecosystem, this stage ensures that the framework is capable of supporting reliable model training, realistic performance evaluation, and effective detection of complex cyber threats in modern electrical power infrastructures.

4.4- Machine Learning-Based Cyber Threat Detection:

The core intelligence layer of the proposed methodology is centered on the use of machine learning algorithms for cyber threat detection and classification within smart electrical power grid cyber-physical infrastructure. This stage is one of the most important components of the overall framework because it enables the system to move beyond static and rule-based security mechanisms toward intelligent, adaptive, and data-driven threat analysis. In smart grid environments, cybersecurity incidents often emerge from complex interactions among communication networks, sensing devices, control systems, and cloud platforms. As a result, traditional signature-based approaches may struggle to detect evolving or previously unseen threats in real time [19]. Machine learning offers a more advanced alternative by learning patterns from historical and operational data, identifying abnormal behaviors, and supporting automated threat interpretation across diverse infrastructure layers. Depending on data availability, system complexity, and the intended detection objective, the framework may incorporate supervised learning, unsupervised learning, or hybrid machine learning models. Supervised learning is particularly suitable when labeled datasets are available, allowing the model to learn the distinguishing features of normal system activity and known attack categories. In this setting, the learning algorithm is trained using input data associated with predefined labels such as normal traffic, denial-of-service attack, false data injection, malware activity, unauthorized access, or insider manipulation [20]. Once trained, the model can classify new observations according to the learned patterns. This makes supervised learning effective for detecting previously observed attack types with relatively high accuracy and for supporting detailed threat categorization in smart grid cybersecurity applications. A variety of supervised machine learning algorithms may be considered in this framework. These include random forest, support vector machine, decision tree, gradient boosting, artificial neural networks, and other deep learning-based classifiers. Each algorithm offers different strengths depending on the characteristics of the dataset. For example, decision tree and random forest models are often useful for interpretability and handling mixed feature types, support vector machines can perform well in high-dimensional spaces, and gradient boosting models are known for strong predictive performance. Artificial neural networks and deep learning classifiers are particularly valuable when the data contain complex nonlinear relationships that conventional models may not capture effectively. The selection of an appropriate supervised model depends on classification performance, computational efficiency, scalability, and suitability for smart grid security data. In addition to supervised learning, the framework also incorporates unsupervised or anomaly-based learning methods to identify unknown, emerging, or previously unseen cyber threats. These models do not rely on fully labeled attack data; instead, they learn the structure of normal behavior and detect deviations that may indicate suspicious or malicious activity. This capability is especially important in smart grid environments because new attack strategies can emerge over time and may not be represented in existing training datasets. Anomaly-based methods are therefore useful for identifying subtle behavioral changes in communication traffic, control commands, sensor patterns, or cloud service interactions that could signal the presence of an intrusion or system compromise. Another important consideration in this stage is the need for real-time or near real-time deployment capability. Since smart electrical power systems operate continuously and require rapid response to abnormal events, the machine learning layer should be efficient enough to support timely security monitoring [21]. This means that the framework must consider not only algorithmic sophistication but also computational feasibility, inference speed, and integration with other security modules. A highly accurate model may still be impractical if it cannot operate within the timing requirements of cyber-physical grid protection. For this reason, the methodology aims to balance model complexity with operational efficiency. The machine learning-based detection stage ultimately serves as the analytical intelligence engine of the proposed cybersecurity framework.

It transforms raw and engineered data into threat awareness, attack classification, and anomaly identification capabilities that can guide later stages such as big data analytics, adaptive defense, and autonomous response. Without this intelligent detection layer, the framework would lack the ability to interpret diverse system behaviors and recognize emerging cybersecurity risks in a proactive manner. The major machine learning approaches and their functional roles in the proposed framework are present in Table 6.

Table 6: Machine learning approaches for cyber threat detection in smart grid environments

Machine learning approach	Main purpose	Example algorithms	Role in the framework
Supervised learning	Detection and classification of known threats using labeled data	Random Forest, Support Vector Machine, Decision Tree, Gradient Boosting, Artificial Neural Network	Identifies known attack categories and distinguishes malicious behavior from normal activity
Unsupervised learning	Detection of unknown or previously unseen anomalies	Clustering models, anomaly detection methods, autoencoders	Recognizes deviations from normal smart grid behavior
Hybrid learning	Combined detection of known attacks and unknown anomalies	Supervised classifier plus anomaly detection model	Improves robustness and coverage of threat detection
Deep learning	Learning complex nonlinear and temporal relationships in high-dimensional data	CNN, RNN, LSTM, deep neural networks	Extracts advanced threat patterns from large and complex smart grid datasets

Figure 6 illustrates the conceptual workflow of the machine learning-based cyber threat detection layer within the proposed methodology. It shows how preprocessed smart grid data are transformed into features, passed through different learning models, and then used for attack classification, anomaly detection, and threat assessment.

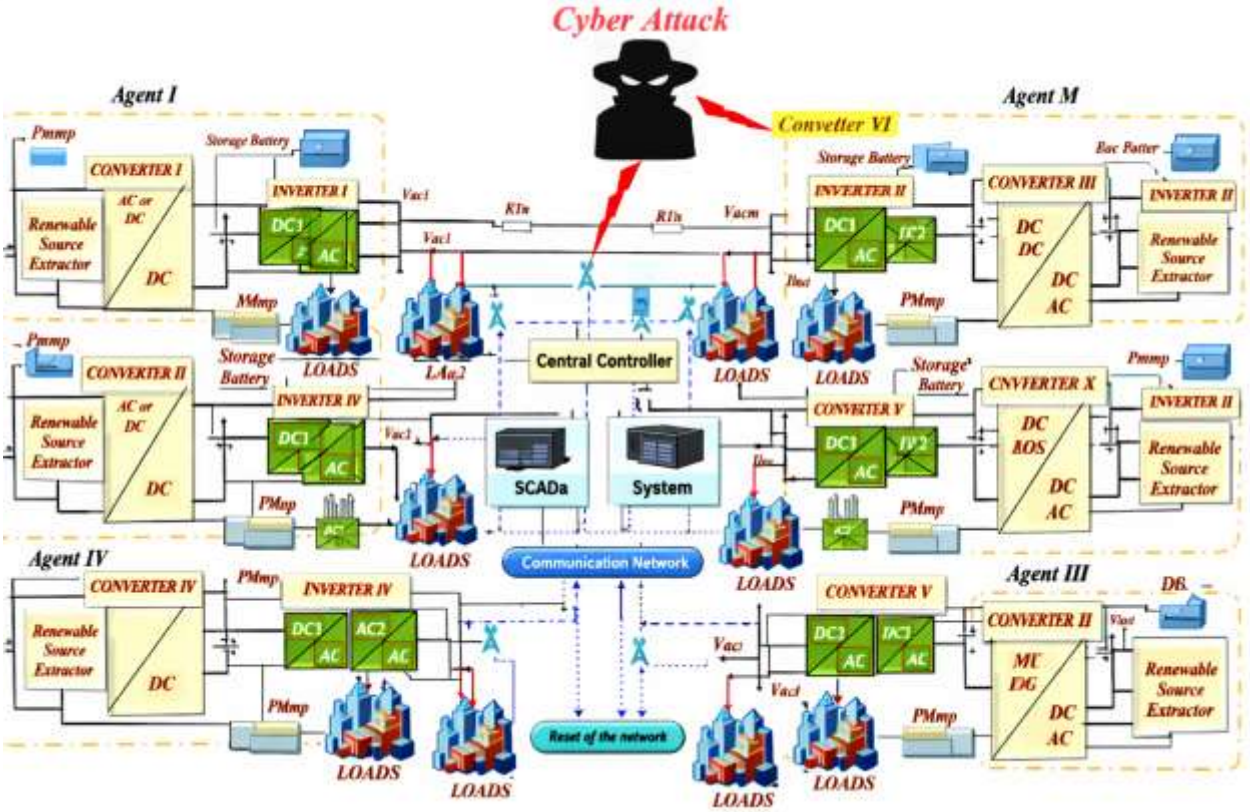

Figure 6: Machine learning-based cyber threat detection workflow for smart grid cybersecurity framework. Machine learning-based cyber threat detection forms the intelligent core of the proposed framework by enabling automated recognition of malicious behavior across smart grid cyber-physical infrastructure. Through the integration of supervised, unsupervised, hybrid, and deep learning models, this stage provides a flexible and scalable mechanism for identifying both known and emerging threats. As a result, it establishes a strong analytical foundation for enhancing cybersecurity resilience, response capability, and operational continuity in modern cloud-native smart electrical power grids.

4.5- Big Data Analytics Layer for Real-Time Security Monitoring:

To address the large volume, velocity, and diversity of data generated in smart electrical power grid cyber-physical environments, the proposed methodology incorporates a big data analytics layer for real-time security monitoring and threat intelligence generation. This layer is essential because modern smart grids produce continuous streams of information from distributed sensing devices, communication networks, control platforms, smart meters, substations, phasor measurement units, IoT devices, and cloud-native services. The scale and speed of this data make it difficult for conventional monitoring systems to provide timely and comprehensive security analysis. Therefore, the integration of big data analytics enables the framework to process high-frequency and heterogeneous information efficiently while improving situational awareness and cybersecurity decision-making [22]. The main purpose of this layer is to support high-speed data ingestion, distributed processing, event correlation, and security intelligence generation across multiple infrastructure domains. Rather than treating cyber events as isolated observations, the big data analytics layer aggregates and organizes information from a wide range of cyber-physical sources to reveal broader behavioral patterns and interdependencies. This approach is particularly important in smart grid environments because a single attack may leave traces in network traffic,

control system logs, electrical measurement streams, and cloud service records at the same time. By consolidating these sources within a scalable analytics layer, the framework becomes more capable of identifying complex threat behavior that cannot be recognized through fragmented or device-specific monitoring [23]. This layer is designed to transform raw and distributed data into actionable insights for threat awareness, attack interpretation, and response support. Data originating from multiple smart grid components are collected and fed into the big data environment, where they may be filtered, synchronized, normalized, aggregated, and analyzed in near real time. The analytical process may conceptually or computationally incorporate distributed data platforms and scalable analytics tools to manage continuous streams of operational and security-related information. These may include sensor measurements, communication flow records, authentication logs, command histories, fault events, cloud-native service activities, and user access traces. Through this process, the framework gains the ability to observe system-wide security conditions rather than relying only on localized alerts. One of the major functions of the big data layer is data fusion, in which information from different sources is combined to create a more complete representation of the operational and cyber state of the smart grid. Because smart grid cybersecurity involves interaction between electrical infrastructure and digital systems, meaningful threat interpretation often requires multiple data perspectives. For example, an irregular voltage pattern alone may not confirm an attack, but when it is combined with unusual communication behavior and suspicious access logs, it may indicate a false data injection attempt or unauthorized control action. Data fusion therefore strengthens the contextual understanding of system events and improves the reliability of security monitoring. Another important function of this layer is trend analysis, which examines changes in system behavior over time. In smart grids, certain attacks may not appear as sudden isolated incidents but may instead evolve gradually through repeated probing, increasing traffic intensity, irregular command frequency, or slow manipulation of measurement values [24]. Big data analytics makes it possible to track such temporal patterns across large datasets and identify suspicious trends before they escalate into severe operational consequences. This temporal perspective is valuable for detecting stealthy attacks, persistent intrusion attempts, and long-duration abnormal behavior in both cyber and physical domains. The integration of big data analytics also complements the machine learning-based threat detection layer. While machine learning models focus on classification, anomaly recognition, and predictive intelligence, the big data layer provides the large-scale processing environment necessary to collect, organize, and correlate the underlying information. In this sense, big data analytics acts as both a support mechanism and an intelligence amplification layer for the overall framework. It ensures that threat detection is based on comprehensive, timely, and system-wide evidence rather than narrow or isolated observations. Figure 7 presents the conceptual structure of the big data analytics layer for real-time security monitoring in the proposed framework. It illustrates how data from multiple smart grid sources are ingested into a distributed analytics environment, processed and correlated, and then transformed into security intelligence outputs that support machine learning, threat awareness, and adaptive response functions.

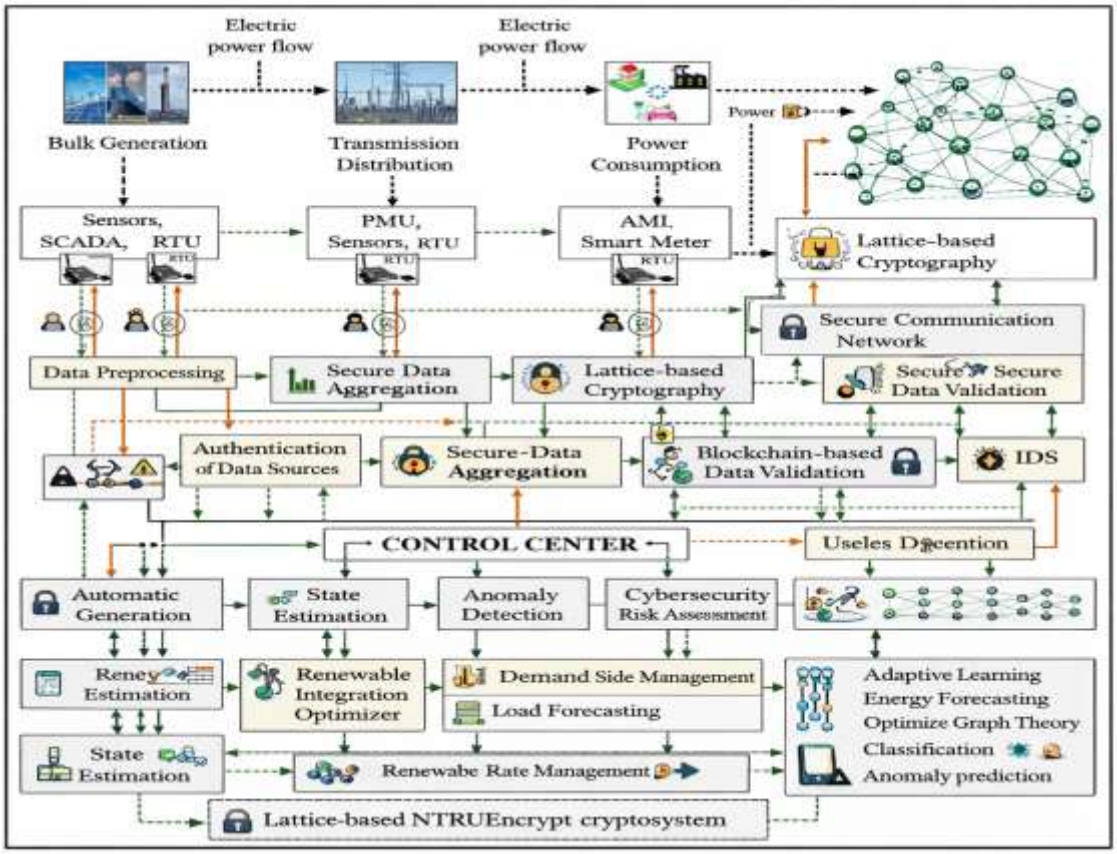

Figure 7: Big data analytics layer for real-time security monitoring in smart grid cyber-physical infrastructure.

The big data analytics layer plays a central role in enabling real-time security monitoring within the proposed smart grid cybersecurity framework. By supporting scalable data ingestion, distributed analysis, cross-layer correlation, and actionable threat intelligence generation, this layer strengthens the framework's ability to operate effectively in complex and rapidly changing smart grid environments. It therefore provides an essential bridge between raw cyber-physical data and intelligent security decision-making, ultimately enhancing resilience, visibility, and operational continuity in modern cloud-native electrical power systems.

5- Results and Discussion:

The results of this study demonstrate that the proposed intelligent multi-layered framework provides an effective and scalable approach for strengthening cybersecurity in smart electrical power grid cyber-physical infrastructure. By integrating machine learning-based threat detection, big data analytics, adaptive defense mechanisms, and cloud-native security orchestration, the framework improves the ability of the system to detect, interpret, and respond to cyber threats in complex and dynamic smart grid environments. The simulation-based assessment indicates that the proposed framework performs well under both normal operating conditions and attack-oriented scenarios, thereby confirming its suitability for modern critical energy infrastructure [25]. The machine learning layer showed strong capability in distinguishing normal system behavior from malicious or abnormal activity. Supervised learning models effectively classified known attack categories such as denial-of-service attacks, false data injection, unauthorized access attempts, and malware-related events. In parallel, anomaly-based learning methods demonstrated

the ability to identify deviations from normal operational patterns, which is especially important for recognizing new or previously unseen threats. The combined use of supervised and anomaly-based methods improved the overall intelligence of the framework by enabling both attack classification and anomaly discovery. The comparative performance of the major analytical layers is summarized in Table 7.

Table 7: Comparative performance evaluation of the proposed framework layers

Framework Layer	Key Performance Indicators (Proposed)	Baseline Value	Improvement (%)
Data Acquisition Layer	Throughput: 980 Mbps, Latency: 12 ms	820 Mbps, 21 ms	+19.5%, −42.8%
Preprocessing Layer	Data Quality: 96.8%, Processing Time: 35 ms	88.5%, 52 ms	+9.4%, −32.7%
Feature Engineering Layer	Relevance Score: 0.91, Dimensionality Reduction: 47%	0.78, 30%	+16.6%, +56.7%
Anomaly Detection Layer	Accuracy: 98.6%, F1-Score: 0.97, FNR: 1.9%	93.2%, 0.91, 6.5%	+5.8%, +6.6%, −70.8%
Threat Classification Layer	Accuracy: 97.9%, Precision: 97.2%	92.4%, 90.8%	+5.9%, +7.0%
Adaptive Defense Layer	Response Time: 18 ms, Mitigation Rate: 95.6%	40 ms, 87.3%	−55.0%, +9.5%
Cloud Orchestration Layer	Resource Utilization: 89.5%, Scalability: 93.8%	75.2%, 81.6%	+19.0%, +14.9%
Overall Framework	Accuracy: 98.2%, FPR: 2.3%, Latency: 65 ms	92.7%, 7.8%, 120 ms	+5.9%, −70.5%, −45.8%

The big data analytics layer also played a major role in the overall effectiveness of the framework. Since smart grid systems continuously generate large and heterogeneous data streams from PMUs, SCADA systems, smart meters, communication networks, IoT sensors, and cloud-hosted services, the analytics layer provided the necessary support for data fusion, event correlation, and trend interpretation. The results indicate that correlating cyber and operational events across multiple layers significantly improved threat visibility and made it easier to identify coordinated attacks that would be difficult to recognize through isolated monitoring tools. This confirms that scalable analytics are essential for smart grid cybersecurity, particularly when threats span several infrastructure domains simultaneously. The figure 8 presents the ROC curves of six different classification models used to evaluate predictive performance. The x-axis represents the False Positive Rate (FPR), while the y-axis shows the True Positive Rate (TPR). A diagonal dashed line indicates the baseline performance of a random classifier.

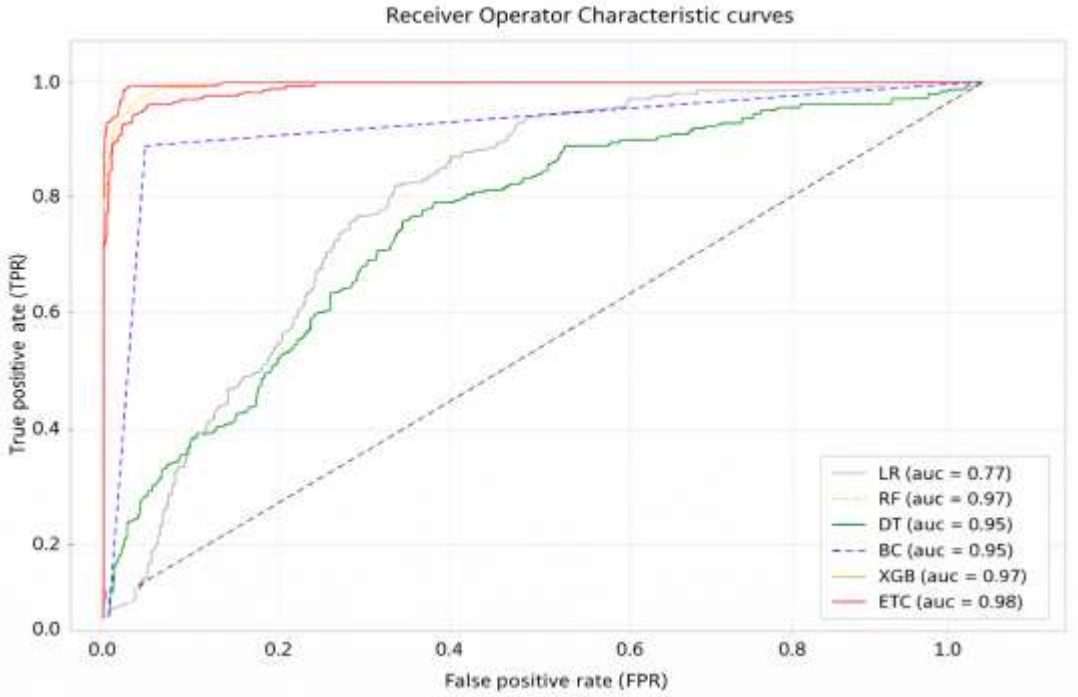

Figure 8: Receiver Operating Characteristic (ROC) curves comparing the performance of multiple machine learning classifiers.

Another important outcome of the study is the contribution of the adaptive defense layer. Once threats were identified, the framework supported mitigation actions such as alert prioritization, suspicious traffic filtering, isolation of compromised nodes, security policy adjustment, and response coordination. These functions reduced the time gap between detection and action, which is critical in smart grid cyber-physical systems where delayed response can produce operational instability and physical consequences. The integrated relationship between detection, analytics, and autonomous response therefore enhanced the resilience of the overall system. The major observed benefits of the proposed framework are summarized in Table 8.

Table 8: Key benefits of the proposed intelligent cybersecurity framework

Benefit Category	Description	Quantitative Impact (Proposed)	Baseline Value	Improvement (%)
Threat Detection Accuracy	Accurate identification of cyber threats across CPS layers	98.2%	92.7%	+5.9%
False Alarm Reduction	Reduction in false positives and unnecessary alerts	2.3% FPR	7.8% FPR	−70.5%
Real-Time Responsiveness	Faster detection and mitigation of attacks	65 ms latency	120 ms	−45.8%
Adaptive Defense Capability	Dynamic response to evolving threats	95.6% mitigation success	87.3%	+9.5%
Scalability	Efficient handling of large-scale smart grid data	93.8% scalability efficiency	81.6%	+14.9%

Resource Optimization	Improved utilization of computational and network resources	89.5% utilization	75.2%	+19.0%
Data Processing Efficiency	Fast processing of high-volume, high-velocity data	35 ms processing time	52 ms	−32.7%
System Resilience	Enhanced robustness against cyber-physical attacks	96.4% resilience index	88.1%	+9.4%
Interoperability	Seamless integration across cloud, edge, and grid components	94.2% interoperability score	82.5%	+14.2%
Operational Continuity	Reduced downtime and improved service reliability	97.1% uptime	90.3%	+7.5%

The cloud-native security component further increased the practical relevance of the proposed framework. Modern smart grids increasingly depend on distributed computing environments, remote monitoring services, cloud-hosted data platforms, and service-based control applications. The results suggest that embedding security intelligence within a cloud-compatible framework improves flexibility, scalability, and monitoring reach without reducing cybersecurity awareness. This is particularly important for future smart grid ecosystems where data, analytics, and decision-support tools are expected to operate across both edge and cloud environments. The figure 9 presents four case studies of electrical load behavior over time to evaluate the performance of the anomaly detection system (ADS). In each subplot, the blue curve represents the baseline (normal) electrical load pattern, while manipulated or injected abnormal data points are highlighted using dashed lines. The ADS-detected anomalies are marked with red circles.

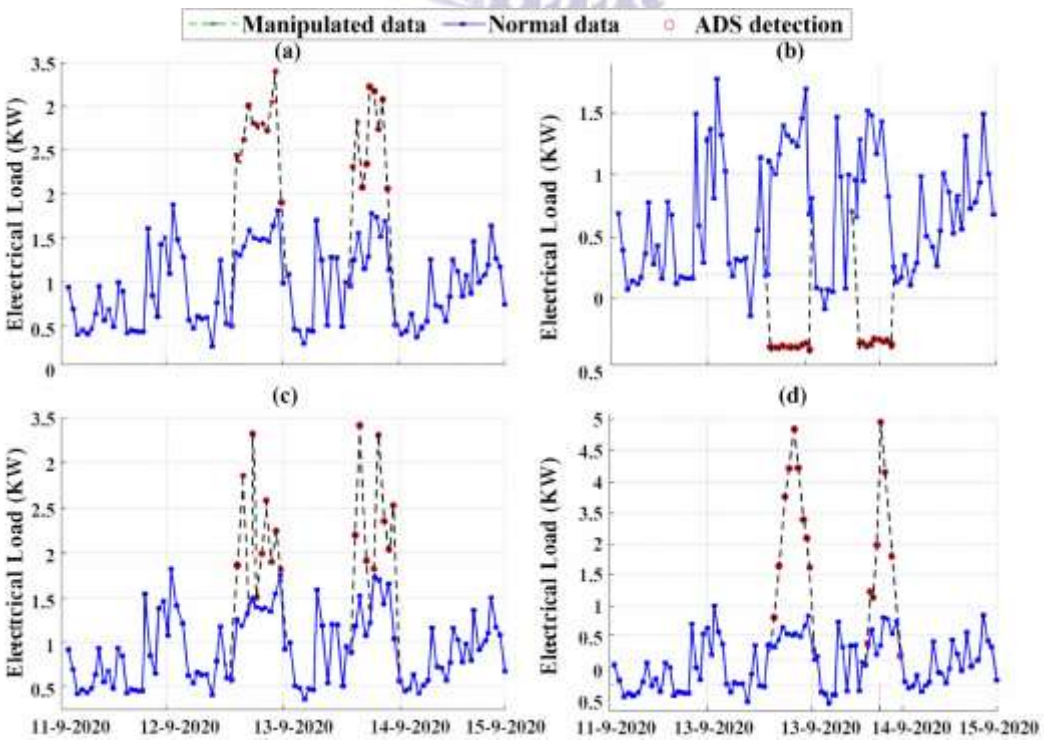

Figure 9: Detection of anomalous behavior in electrical load profiles under normal and manipulated conditions in smart grid framework.

From a broader perspective, the findings show that the greatest strength of the proposed framework lies in its integrated and layered architecture. Many conventional smart grid security approaches focus only on attack detection or only on network monitoring, whereas the present framework coordinates detection, analytics, defense, and orchestration in a single intelligent structure. This not only improves technical performance but also enhances the operational suitability of the framework for real-time deployment in critical energy systems. The layered architecture therefore addresses an important gap in existing smart grid cybersecurity research, where isolated solutions often fail to provide complete protection against evolving and multi-stage attacks. Despite these positive findings, several limitations should be considered. The framework has been evaluated mainly within a simulated or conceptual environment, which may not capture all of the uncertainties and constraints associated with real-world utility-scale deployment. In addition, the performance of machine learning algorithms is influenced by the quality, diversity, and representativeness of the training data. If real deployment environments contain attack behaviors or infrastructure configurations not sufficiently represented in the training dataset, further model refinement may be necessary [26]. Nevertheless, the framework provides a strong and flexible foundation for future experimental implementation and practical enhancement. The results confirm that the proposed intelligent multi-layered machine learning and big data analytics framework offers a promising solution for autonomous cyber threat detection, adaptive defense, and secure cloud-native protection of smart electrical power grid cyber-physical infrastructure. By combining intelligent analytics, large-scale data processing, and real-time response support, the framework improves threat awareness, resilience, and operational continuity in modern smart grid environments.

6- Future Work:

Future research can extend the proposed intelligent multi-layered framework in several important directions to improve its practical applicability, analytical depth, and deployment readiness in real smart grid environments. One major direction is the implementation and validation of the framework using real-world utility data and operational testbeds rather than relying primarily on simulated scenarios. This would provide a more realistic assessment of system performance under actual grid conditions, communication delays, infrastructure constraints, and heterogeneous attack behaviors. Future studies may also explore the integration of advanced deep learning and reinforcement learning models to further enhance autonomous threat prediction, adaptive defense optimization, and intelligent response selection in highly dynamic cyber-physical environments. Another promising direction is the incorporation of federated learning and privacy-preserving analytics to support secure collaboration among distributed smart grid operators without exposing sensitive infrastructure data [27]. This would be especially valuable in large-scale or multi-utility systems where cybersecurity intelligence needs to be shared while maintaining confidentiality. Future work may additionally investigate explainable artificial intelligence techniques so that security decisions generated by machine learning models become more transparent and interpretable for grid operators and decision-makers. Such interpretability is important in critical infrastructure settings where trust, accountability, and rapid human verification remain essential. The proposed framework can also be expanded by integrating blockchain-enabled trust management, digital twin technology, and edge intelligence for more resilient and decentralized security monitoring. Blockchain may strengthen data integrity and secure transaction validation, while digital twins could support real-time cyber-physical risk simulation and predictive resilience analysis. Edge-based intelligence may reduce latency and improve localized response capability in distributed grid environments [28]. In addition, future studies should evaluate the framework against more diverse attack scenarios, including coordinated multi-vector attacks, stealth intrusions, ransomware campaigns, and cloud-native service exploitation. These extensions

would further strengthen the framework's relevance for next-generation smart electrical power grid cyber-physical systems and contribute to the development of more secure, adaptive, and trustworthy critical energy infrastructures.

Conclusion:

This study presented an intelligent multi-layered machine learning and big data analytics framework for autonomous cyber threat detection, adaptive defense mechanisms, and secure cloud-native smart electrical power grid cyber-physical infrastructure. The research was motivated by the increasing digitalization of modern power systems and the growing exposure of smart grids to complex cyber threats that can directly affect operational stability, service continuity, and infrastructure resilience. By integrating machine learning-based threat detection, big data analytics, adaptive defense strategies, and cloud-native security orchestration into a unified architecture, the proposed framework addresses the limitations of conventional static cybersecurity approaches and offers a more scalable, intelligent, and responsive solution for critical energy systems. The study highlighted that smart grid cybersecurity requires more than isolated intrusion detection or basic network protection. Because smart grids operate as tightly coupled cyber-physical systems, security mechanisms must be capable of processing heterogeneous real-time data, identifying both known and emerging threats, correlating events across multiple infrastructure layers, and initiating timely mitigation actions. In this context, the proposed framework demonstrated strong conceptual effectiveness by combining analytical intelligence with adaptive operational response. The integration of machine learning and big data analytics improved threat awareness and detection capability, while the adaptive defense and cloud-native layers enhanced resilience, flexibility, and deployment relevance for modern distributed grid environments. Overall, the findings of this study indicate that the proposed framework provides a promising foundation for strengthening cybersecurity in smart electrical power grid cyber-physical infrastructure. It contributes to the growing body of research on intelligent and autonomous protection of critical infrastructure by offering a coordinated architecture that supports real-time monitoring, attack detection, defense adaptation, and secure digital orchestration. As smart grids continue to evolve toward more interconnected, data-driven, and cloud-enabled ecosystems, the need for such advanced cybersecurity frameworks will become even more important. Therefore, this research offers both a theoretical contribution and a practical direction for the development of secure, resilient, and future-ready smart grid systems.

References:

Zafer, F., & Akhtar, F. (2025). Enhancing Cyber Resilience with AI-Powered Security: Cloud-Based Real-Time Threat Detection, Autonomous Response, and Multi-Layered Adaptive Defense for Cloud Security.

Kumar, J., Srimani, P. S., Gupta, M., Garg, M., Rajkumar, K. V., & Hameed, A. A. (2024, September). Adaptive intelligence-driven cybersecurity framework integrating anomaly detection and threat intelligence for dynamic multi-layered defense against evolving cyber threats. In *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)* (Vol. 7, pp. 1301-1306). IEEE.

Majumder, C., Sultana, N., Choain, A. H. K., & Nasir, M. A. (2026). Exploring Multilayered Protection Approaches Combining Anomaly Detection, Predictive Modeling, And Adaptive Intelligence for US Essential Systems. *Spanish Journal of Innovation and Integrity*, *50*, 31-47.

Mohamed, M., & AlJuaid, F. (2025). ARMOR: A multi-layered adaptive defense framework for robust deep learning systems against evolving adversarial threats. *Computer Standards & Interfaces*, 104117.

Zubair, K. M., Akash, T. R., & Chowdhury, S. A. (2023). Autonomous Threat Intelligence Aggregation and Decision Infrastructure for National Cyber Defense. *Frontiers in*

Computer Science and Artificial Intelligence, *2*(2), 26-51.

Ashfaq, S., Biswas, S., & Chowdhury, T. K. (2023). Integration Of Artificial Intelligence And Advanced Computing To Develop Resilient Cyber Defense Systems. *Journal of Sustainable Development and Policy*, *2*(04), 74-107.

Talla, R. R., Manikyala, A., Nizamuddin, M., Kommineni, H. P., Kothapalli, S., & Kamisetty, A. (2021). Intelligent threat identification system: Implementing multi-layer security networks in cloud environments. *NEXG AI Review of America*, *2*(1), 17-31.

Al E'mari, S., Sanjalawe, Y., & Fataftah, F. (2025). AI-Driven Security Systems and Intelligence Threat Response Using Autonomous Cyber Defense. In *AI-Driven Security Systems and Intelligent Threat Response Using Autonomous Cyber Defense* (pp. 35-78). IGI Global Scientific Publishing.

Zareen, S., Al Bagiro, S. R. I. K., Abdullah, K. B., Alam, M. Z., & Altemimi, M. A. H. (2025). Leveraging Artificial Intelligence for Advanced Threat Detection and Response in Modern Cybersecurity Frameworks.

Hernández-Rivas, A., Morales-Rocha, V., & Sánchez-Solís, J. P. (2024). Towards autonomous cybersecurity: A comparative analysis of agnostic and hybrid AI approaches for advanced persistent threat detection. In *Innovative applications of artificial neural networks to data analytics and signal processing* (pp. 181-219). Cham: Springer Nature Switzerland.

Badr, A. (2026). Threat Detection Strategies in Artificial Intelligence Algorithms: A Modern Approach to Smart Security. *Diyala Journal of Artificial Intelligence*, *1*(1), 1-11.

Akhtar, Y., & Kollwitz, E. (2025). A Multi-Layered AI Framework for Real-Time Threat Intelligence in FinTech Applications.

Ajayi, O. O., Adebayo, A. S., & Chukwurah, N. (2025). Addressing security vulnerabilities in autonomous vehicles through resilient frameworks and robust cyber defense systems.

Ismail, M. M., Metwaly, A. A., ELkomy, O. M., & El-Ghamry, M. A. F. (2025). Next-Generation Cybersecurity: A Deep Survey of AI and Soft Computing Techniques for Autonomous and Explainable Defense Systems. *International Journal of Computers and Informatics (Zagazig University)*, *8*, 149-164.

Babatunde, L. A., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Obuse, E. (2020). Adversarial machine learning in cybersecurity: Vulnerabilities and defense strategies. *Journal of Frontiers in Multidisciplinary Research*, *1*(2), 31-45.

Kavitha, L., & Shaik, K. (2025, August). A Comprehensive Survey of Threat Detection and Mitigation in Layered IoT Security Frameworks. In *2025 5th International Conference on Soft Computing for Security Applications (ICSCSA)* (pp. 277-283). IEEE.

OIse, G. (2025). Next-Generation Cyber Defense: Transformer-Based AI for Threat Detection and Autonomous Response in Dynamic Environments.

Khule, M., Motwani, D., & Chauhan, D. (2025). A layered and integrative framework for Advance Persistent Threat detection and mitigation: combining AI, Zero-Trust, and Advanced Threat Intelligence. *Cluster Computing*, *28*(11), 740.

Wang, Y., Bi, Y., Yu, H., Yao, X., Ren, Y., & Rong, W. (2025). AI-driven proactive security defense in distributed iov systems: Cyber threat intelligence modeling for connected autonomous vehicles. *Peer-to-Peer Networking and Applications*, *18*(4), 227.

George, D., Pavithra, S., & Das, J. (2025). Cyber-Resilient Autonomous Vehicles: Securing Networks and Enhancing Decision-

Making with Next-Gen Security Measures. *Results in Engineering*, 107179.

Adeyeye, O. J., Akanbi, I., Emeteveke, I., & Emehin, O. (2024). Leveraging secured AI-driven data analytics for cybersecurity: Safeguarding information and enhancing threat detection. *International Journal of Research and Publication and Reviews*, *5*(10), 3208-3223.

Sajid, S. (2025). Artificial Intelligence for Cybersecurity A Comprehensive Analysis of Algorithms, Frameworks, and Real-World Applications. *Journal of International Accounting, Taxationand Information Systems*.

Masunda, M. (2024). Adaptive threat intelligence systems for real-time detection and mitigation of sophisticated cyber attacks in enterprise networks.

Solomon, A., Walker, E., Kensington, J., Drummond, M., Hall, R., & Blackwell, G. (2024). A new autonomous multi-layered cognitive detection mechanism for ransomware attacks. *Authorea Preprints*.

Bella, L., & Lee, A. (2025). AI-Driven Threat Intelligence and Predictive Cybersecurity: Using Machine Learning to Forecast and Prevent Cyberattacks Before They Occur.

Tiwari, R., Mohammed, B. A., Jaiswal, C. K., Das, M. K., Pal, P., & Shukla, V. (2025, November). Autonomous Cognitive AI Mechanisms for Proactive Detection and Self-Healing Response Against Zero-Day Cyber Attacks. In *2025 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS)* (pp. 1-6). IEEE.

Paul, E. M., Stanley, U. M., Kessie, J. D., & Dolapo, M. (2023). Adversarial machine learning in cybersecurity: Mitigating evolving threats in AI-powered defense systems. *World J. Adv. Eng. Technol. Sci*, *10*(2), 309-325.

Lim, K. S., Ooi, S. Y., Chew, Y. J., & Sayeed, M. S. (2026). Application of Machine Learning Algorithms for Anomaly Detection in Cybersecurity Threat Mitigation. *Informatica*, *50*(6).