IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security Measures In Smart Electric Grids: A Machine Learning Review

Priyamvada Chandel
Joint Director, CPRI Bhopal, MP India

Abstract: As smart grid systems continue to evolve through the integration of advanced communication technologies and an increasing number of interconnected devices, the imperative for robust cybersecurity measures has become paramount. This study examines the current state of smart grid cybersecurity, emphasizing the challenges arising from heterogeneous environments and the integration of Internet of Things (IoT) components. It investigates various machine learning methodologies designed to enhance threat detection, response capabilities, and overall system resilience. Furthermore, this study identified significant deficiencies in the existing architecture, particularly regarding protocol compatibility and data aggregation security. To address these issues, a novel proposal for a unified IPv6-based communication layer is introduced, which simplifies connectivity, mitigates security vulnerabilities, and facilitates direct Internet access for all devices. This framework not only improves the efficiency of data transmission but also strengthens the security posture of smart grids through the implementation of IP-based security protocols. These findings underscore the necessity of advancing cybersecurity measures in smart grids and delineate future research directions aimed at developing comprehensive strategies to ensure the integrity and resilience of this critical infrastructure against evolving cyber threats.

***Index Terms*:** Cyber Security, Information and Communication Technologies (ICT), Internet of Things, Networks, and Smart Grid.

1. INTRODUCTION

The global transition towards smart grids represents a significant milestone in the modernization of energy infrastructure, combining the traditional power grid with advanced information and communication technologies (ICT).This fusion allows for more efficient and sustainable management of electricity, particularly with the integration of distributed renewable energy sources near areas of consumption [1-2]. As energy systems evolve, smart grids introduce bidirectional power flows that enable dynamic energy exchange between utilities and consumers through sophisticated two-way communication networks [3-5]. This shift away from a centralized, utility-owned grid creates new opportunities for innovation and collaboration among a wide range of stakeholders. The National Institute of Standards and Technology (NIST) conceptual model highlights the complexity of the smart grid by identifying seven key sectors: large-scale power generation, transmission, distribution, consumption, service providers, operations, and markets [6-8]. By leveraging these components, smart grids can achieve high levels of efficiency, resilience, and flexibility in terms of energy management.

Additionally, companies such as IBM have developed advanced models for smart grids, which provide further insights into the role of computing platforms, data storage, and communication infrastructure. These models emphasize the importance of scalable technologies such as Software as a Service (SaaS) and Infrastructure as a Service (IaaS) in supporting device connectivity, while addressing crucial factors such as protocol capacity, resilience, bandwidth, latency, and security [9]. Through these advancements, smart grids have paved the way for a more responsive and sustainable energy future.

The smart grid's architecture is built on multiple layers, each serving distinct functions to ensure efficient operation and integration, as shown in Figure 1.

- **Software Layer:** This layer includes tools for evaluating meter data, managing billing, monitoring outages, controlling overloads, and integrating devices for both field technicians and users. It also incorporates geographic information systems (GIS), wide-area management systems, and customer information systems.
- **System Integration Platform:** The system integration platform handles the coordination of applications and data, network and security management, and computing frameworks necessary for grid operation.
- **Communication Layer:** This layer consists of various communication networks, including centralized, office, external, access,and black hole networks, as well as in-home, neighborhood, and central networks. It supports both wired and wireless communication across short and long distances.
- **Physical Layer:** The physical layer encompasses energy production, distribution, transmission, consumption, renewable energy sources, and energy storage systems within the smart grid.

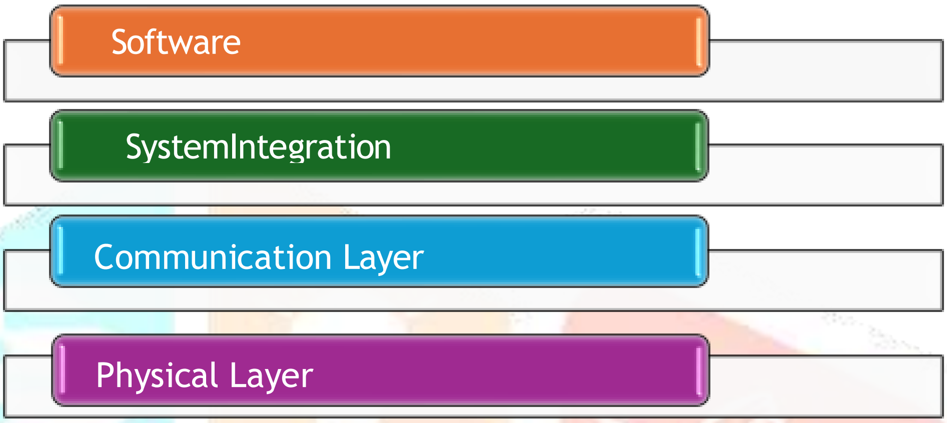

Figure 1: Conceptual Framework for Smart Grid

In the framework of the NIST conceptual model, Figure 1 replicates the IBM model [9], showing that approximately 70% of the smart grid infrastructure consists of Information and Communication Technology (ICT) layers [10].

A detailed examination of the communication layer revealed that multiple wired and wireless networks are essential for connectivity across various distances. The software layer further integrates tools for managing grid operations, requiring access for different user groups, such as operators, home owners, field engineers, service providers, and marketing staff. However, the widespread access inherent in these systems introduces significant cybersecurity risks. To mitigate these threats, strong permission and authentication mechanisms are necessary to protect the grid from unauthorized intrusions.

1.1 Uses of Machine Learning Techniques for Cyber Security of Smart Grid

Machine learning (ML) methods are often categorized based on their various applications within smart grids (SGs), although they do not always focus on cyber security, or by their learning types (e.g., supervised, unsupervised, and reinforcement learning). The works thus far typically highlight the limitations, benefits, and drawbacks in detail. While some mention future directions, they often do not address the specific area of interest. In this regard, it is essential to provide clear, actionable guidelines on "how to implement" solutions. Furthermore, most studies do not offer specific recommendations on model selection or reconstruction, nor do they explain the criteria for choosing a particular ML model.

To address these gaps and offer a more focused evaluation of ML applications in SG cyber security, this study focuses on the following:

- Presenting a comprehensive solution to "how to solve attack detection problems" using ML tools, thus addressing model selection challenges.
- Developing a flowchart that provides guidance on "which criteria to use for selecting a specific ML model," making it easier to choose the appropriate model based on different data characteristics.
- Offering an enhanced classification of ML models focused on SG cyber security, improving on previous efforts by ranking ML tools according to the CIA (Confidentiality, Integrity and Availability) security model to provide a clearer application of ML techniques to SG security challenges.
- We provide a categorization of ML models by complexity—comparing conventional learning and deep learning—to clarify the different levels of complexity in data handling.
- It covers all earning paradigms, including supervised, unsupervised, and reinforcement learning, and discusses modeling approaches, such as traditional, hybrid, and ensemble methods.
- Compile a list of datasets, systems, and types of attacks to quickly locate relevant applications and common security threats.
- Summarize the benefits, drawbacks, and challenges of ML-based cybersecurity approaches in power grids.
- The key areas for future research are highlighted.

This study was based on a thorough literature search, focusing on recent studies from the past five years, with particular emphasis on the most relevant papers published in the last three years from major databases. The proposed model and identified drawbacks are both derived entirely from a review of the existing literature. Carefully chosen keywords related to ML and cyber security in smart grids were used to guide this search. The analysis indicates that most studies concentrate on detecting attacks, with relatively few addressing mitigation or correction measures. It is important to note that this focus on detection reflects the trends in the papers analyzed, rather than an intentional bias toward that area.

1.2 Goals and Requirements for Protection

The smart grid comprises numerous interconnected devices that share two primary types of data: informational and operational. Informational data include power usage bills, trends, logs, tags, historical reports, geographic locations, customer information, and emails [11].Operational data, on the other hand, include real-time voltage and current readings, transformer tap positions, capacitor banks, transformer feeder loads, fault locations, relay statuses, and circuit breaker conditions [12-13].Owing to its critical nature, operational data requires a high level of security to protect the smart grid from potential threats and vulnerabilities that could lead to blackouts.

The key protection objectives and requirements for the smart grid are as follows:

- **Availability**: Ensuring timely access to information within the smart grid. Lack of availability could prevent authorized users from accessing the system, potentially disrupting power delivery. Denial of Service (DoS) attacks, which aim to disrupt data transmission and make resources inaccessible, target system availability.
- **Integrity:** Preventing unauthorized changes to data or systems. A loss of integrity in the smart grid can alter the process values or sensor readings, negatively impacting power management.
- **Confidentiality:** Restricting access for unauthorized individuals to safeguard personal privacy and security. Smart grid networks transmit data with varying levels of sensitivity, ranging from consumption statistics to private customer information.
- **Authentication:** Verifying the true identity of the parties involved in communication. Both human and machine authentication are crucial, as breaches can allow hackers access to private data or unauthorized devices to exploit smart grid resources.

- **Authorization:** Managing access to systems and data, known as access control. An authorization system is essential in a smart grid to handle a wide variety of devices and users, ensuring proper access to data and resources.
- **Non-Repudiation:** Ensuring that actions taken by a system or user cannot be denied later. This is particularly important when sensitive information and valuable resources are involved.

2. SECURITY GAPS AND SOLUTIONS IN THE SMART GRID

2.1 Security Gaps in Smart Grid

Smart grids face several risks and challenges, particularly in terms of cybersecurity. This section explores various security concerns and the techniques employed to safeguard smart grid systems.

- **Connectivity:** The smart grid communication network is highly intricate, incorporating a wide range of compatible devices. Owing to their decentralized nature, these systems require robust defenses against potential attacks and vulnerabilities. Such attacks can give attackers control over the grid, leading to physical harm, blackouts, and decreased efficiency [14].
- **Trust:** The interconnected nature of smart grid systems has led to a shift in design principles, moving away from assuming that all consumers can be trusted. Some users may deliberately cause harm, such as tampering with smart meters to report incorrect power consumption data at lower costs.
- **Customer Privacy:** Preserving customer privacy is critical in any system, including smart grids. The deployment of smart meters raises privacy concerns, as they can potentially expose sensitive information about users' daily routines and home presence. This information can be exploited by criminals, companies, marketers, or competitors. Therefore, it is crucial to safeguard user privacy during data transmission and storage.
- **Software Flaws:** Smart grids are vulnerable to software flaws, including malware. Malicious software or updates targeting Supervisory Control and Data Acquisition (SCADA) systems pose a significant threat. Such systems often exhibit well-known vulnerabilities that require patching. However, the high costs and potential downtime associated with patching make it difficult for critical systems such as smart grids [15].

2.2 Techniques for Securing Smart Grid Systems

Cyber security in smart-grid systems is a topic of great interest to researchers and industry professionals. Although some solutions have been proposed, numerous vulnerabilities persist. This section examines current strategies to address cyber security issues in smart grid technologies.

2.2.1 Cyber Security on Networks

One of the most common attacks on smart grid networks is the denial of service(DoS) attack, which aims to disrupt the normal operations of the target system. To defend against such attacks, smart-grid systems employ various detection and mitigation techniques [16].

A. Detection of DoS

Smart grid systems must detect DoS attacks in real time to implement appropriate defenses, especially against Distributed Denial of Service (DDoS) attacks. Methods for detecting DoS attacks include the following:

- **Flow Entropy Method:** Analyzing network traffic and measuring flow entropy to identify abnormal behavior indicative of a DoS attack [17-19].
- **Signal Intensity Analysis:** Assessing energy levels to detect jamming attempts in wireless networks [20].
- **Sensing Time Measurement:** Using Carrier Sense Multiple Access (CSMA)to detect unusually long channel sensing times, which may indicate a jamming attack [21].
- **Transmission Failure Count:** Monitoring transmission errors to detect jamming attacks based on a failure threshold [21].
- **Signature Detection:** Matching known attack behaviors and characteristics to detect DoS attacks [20].

B. DoS Mitigation

Mitigating DoS attacks involves network and physical layer strategies.

- **Pushback:** Sending attack information to upstream routers to block malicious traffic [20].
- **Rate Limiting:** Reduces data transmission rates of suspicious users [20].
- **Filtering:** Blocking packets from black-listed IP addresses [20].
- **Reconfiguration:** Network topology is adjusted to allocate more resources to victims or isolate attackers [20].
- **Cleaning Center:** Rerouting traffic through a specialized node that filters and handles potential attacks [20].

At the physical layer, techniques such as Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DS), and Chirp Spread Spectrum (CSS) are used to counteract frequency jamming attacks. These methods spread data across multiple frequencies to protect against interference [22-23].

2.2.2 Information Security

Securing data and authenticating devices is another critical aspect of protecting smart grid networks. Encryption techniques such as public-key encryption and symmetric-key encryption are used to protect user information and communications. Public key encryption provides better security, whereas symmetric encryption is more efficient for devices with limited processing power.

Authentication must also be efficient, fault-tolerant, resilient to attacks, and support multicast communication, which is essential for smart grids. Various techniques for multicast authentication include secret information asymmetry, time asymmetry, and hybrid asymmetry.

2.2.3 Key management

Effective key management is crucial for maintaining encryption and authentication in a smart grid. This includes symmetric key management and public key infrastructure (PKI). PKI verifies the authenticity of communicating parties using certificates, whereas symmetric key management handles the creation, distribution, storage, and updating of keys. Scalability, efficiency, and resolvability are key factors for managing keys in a vast smart-grid network [6].

2.2.4 Network security protocols

Creating secure network frameworks and protocols is essential for smart grid security. Many smart grid systems rely on internet-based protocols such as TLS and IPSec. Additionally, secure protocols tailored to smart grid requirements, such as Secure DNP3, IEC61850, and IEC62351, are used to enhance communication security.

Smart grid networks typically use one of two architectures for secure infrastructure:

- Trust-based architecture: Devices authenticate each other by assigning trust levels.
- Role-based network architecture: Devices are assigned roles and permissions within specific domains.

2.2.5 Compliance audits

Compliance audits are conducted using automated tools to assess each system component and ensure that configurations meet security standards. These tools help identify potential vulnerabilities, which are critical in preventing security breaches in vital systems such as smart grids [24].

By addressing these security gaps and implementing robust solutions, smart grids can become more resilient to cyber threats, thereby ensuring the safe and efficient operation of modern power systems.

3. Role of Machine Learning Techniques in Cyber Security

3.1 Cyber-Attack Types and Frequency in Smart Grids

The smart grid ecosystem is complex and dynamic, integrating various communication and control systems to ensure efficient energy distribution. However, with this level of connectivity, there is a significant vulnerability to cyber-attacks. The types of cyber-attacks that target smart grids vary in terms of sophistication, impact, and frequency. To better understand these threats, analyzing the distribution of cyber-attacks that have historically affected smart grids is essential.

3.1.1 Cyber-Attack Distribution in Smart Grids

The chart below represents the distribution of the different types of cyber-attacks commonly encountered in smart grids in Figure 2.

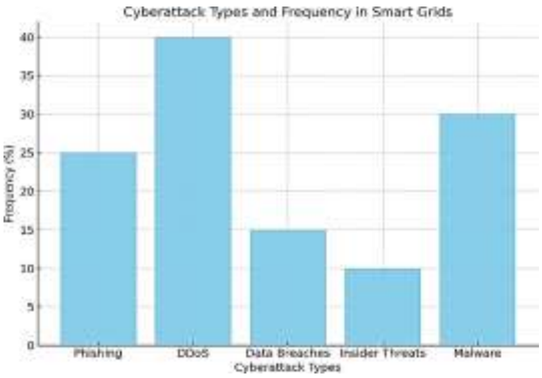

Figure 2. Different Cyber-Attacks in Smart Grid

As illustrated, DDoS attacks represent the most frequent type of attack, accounting for 40% of incidents, followed by malware attacks at 30%. Phishing, data breaches, and insider threats occur less frequently but remain significant threats. These attack types target the grid's critical infrastructure with the aim of disrupting operations or stealing sensitive information.

3.1.2 Attack Types:

- **DDoS (Distributed Denial of Service) Attacks**: These overwhelm grid communication networks, disrupting services and impairing the grid's operational capacity.
- **Malware**: This infiltrates control systems, allowing unauthorized access to grid data and control mechanisms.
- **Phishing**: Exploits human errors, often targeting employees to gain access to grid control systems.
- **Data Breaches**: Targets sensitive customer or operational data, leading to privacy concerns and operational risks.
- **Insider Threats**: Involve malicious actions by trusted personnel within the grid ecosystem, often resulting in more sophisticated, hard-to-detect compromises.

This distribution highlights the importance of multilayered security solutions and machine learning models that can dynamically respond to a variety of threats, ensuring the resilience of the smart grid against cyber-attacks.

This survey underscores the need for advanced cyber security strategies, integrating real-time detection mechanisms, robust authorization protocols, and machine learning models to anticipate and mitigate these cyber threats

3.2 Machine Learning Techniques In Cyber Security

In the past decade, machine learning (ML) techniques have become pivotal in enhancing the cyber security of smart grids. Researchers have implemented various algorithms to effectively detect and mitigate cyber threats. The chart in Figure 3 highlights the growing use of prominent machine learning models, such as Support Vector Machines (SVM), Random Forests, and Deep Learning, from 2015 to 2024, based on surveyed studies.

The chart shows a steady increase in the application of these techniques over time.

- **SVM**: Initially popular for its effectiveness in classification, SVM usage saw significant growth until 2020, after which it stabilized.
- **Random forests**: Their ability to handle large datasets and provide accurate predictions has led to consistent growth, making them one of the preferred models by 2024.
- **Deep learning**: As data complexity and volumes have increased, deep learning has become the dominant approach from 2020 onward, particularly with advancements in neural networks.

This analysis illustrates the trend towards more complex and data-driven models, indicating that future smart grid cyber security will likely rely more heavily on deep learning techniques, driven by their superior performance in detecting sophisticated attacks.

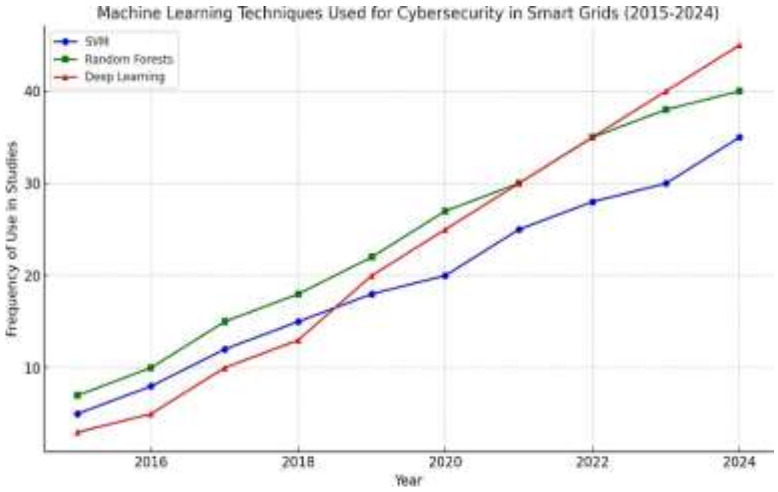

Figure 3. Machine Learning Techniques Used for Cyber Security in Smart Grids (2015-2024)

This section outlines the historical evolution of machine learning models in securing smart grids, emphasizing the need for scalable and adaptable models to address the emerging cyber security challenges.

3.3 Comparison of Detection Rates by Algorithms

Accurate detection of cyber-attacks is critical for maintaining the security of smart grids. Different machine learning algorithms exhibit varying degrees of accuracy in detecting these attacks. The bar chart below compares the detection accuracy rates of several machine learning models applied to smart grid cybersecurity tasks (Figure 4).

- **Deep Learning**: Achieving the highest detection accuracy at 95%, deep learning models are particularly effective in identifying complex and evolving threats owing to their ability to learn from large volumes of data.
- **Random Forests**: With accuracy rate of 90%,random forests are highly effective in detecting cyber-attacks, especially those involving structured data.
- **SVM (Support Vector Machines)**: While SVM performs well, achieving an 85% accuracy rate, it is less effective compared to more advanced models such as deep learning.
- **KNN (K-nearest neighbors)**: At 80%, KNN provides moderate accuracy but struggles with large, high-dimensional datasets.
- **Naive Bayes**: With the lowest detection accuracy of 75%, Naïve Bayes is less capable of handling complex attack patterns but remains useful for simpler classification tasks.

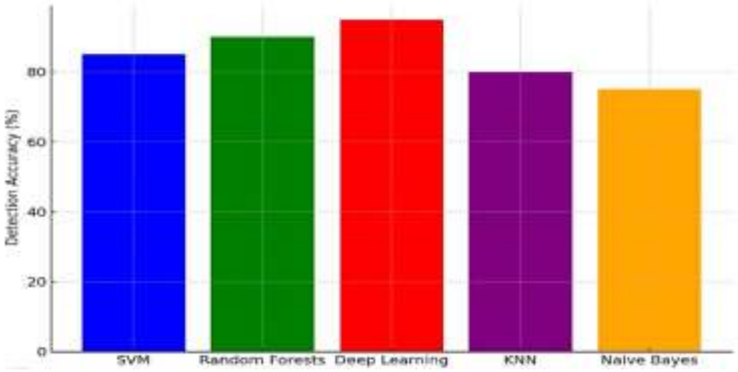

Figure 4.Detection Accuracy Rates of Machine Learning Models

This comparison highlights that while traditional models such as SVM and Naïve Bayes still have their place, more advanced techniques such as deep learning and random forests are increasingly favored for cyber security applications in smart grids owing to their superior detection capabilities.

3.4 Comparison of Different Existing Works

An overview of the work done on machine learning techniques and their application in enhancing cyber security for smart grids is provided in Table 1. Each study addressed different aspects of smart grid security, such as anomaly detection, intrusion detection systems (IDS), and attack prevention.

Table1. Work done on Machine Learning Techniques for Smart Grid Cyber Security

S. No.	Ref.	Year of Publication	Method Used	Description	Limitations
1	27	2020	Anomaly Detection, IDS, Classification Algorithms	A comprehensive review of ML techniques for securing smart grids focusing on anomaly detection and IDS.	Limited to traditional ML models without discussing recent advancements.
2	28	2013	Machine Learning Techniques	Discusses specific cyber security challenges in smart grids and ML-based solutions for cyber-Attack detection.	Focused mainly on case studies, lacks in-depth comparison of Modern ML methods.
3	29	2015	Intrusion Detection Systems (IDS)	Reviews ML-based IDS for real-time data analysis and attack prevention in smart grids.	Does not address deep learning or hybrid models.
4	30	2016	Machine Learning Techniques	Outlines current cyber security threats to smart grids and Explores ML techniques to counter them.	Future research directions are suggested, but lacks practical Implementation details.
5	31	2018	Deep Learning (CNNs, RNNs)	Focuses on deep learning methods for attack detection in smart grid communication and power layers.	More focus on deep Learning ; traditional models not covered.
6	32	2021	Supervised and Unsupervised Learning	Evaluates supervised and unsupervised learning strategies for securing data transmission in smart grids.	Mainly discusses Attack detection Without addressing scalability.
7	33	2020	Decision Trees, SVMs, Neural Networks	Covers various ML techniques for anomaly detection in smart grids to identify potential threats.	Does not explore hybrid or ensemble models.
8	34	2019	Machine Learning- based Intrusion Detection	Surveys ML-based cyber security measures for securing smart grid communication and preventing insider threats.	Focuses on specific attack types, lacks coverage on broader threat landscape.
9	35	2023	Machine Learning- based Intrusion Detection Systems	Explores ML techniques for intrusion detection in smart grids and outlines future directions for enhanced Cyber security.	Needs practical implementation and validation on large-scale datasets.
10	36	2022	Deep Reinforcement Learning	Investigates the use of DRL for mitigating cyber-attacks on smart grids and proposes a DRL-based security framework.	Limited evaluation in real-world smart grid scenarios.
11	37	2022	Block chain and Machine Learning	Comprehensive review of integrating block chain and ML for smart grid Cyber security, emphasizing data integrity.	Lacks empirical comparison between block chain and traditional security

					methods.

Shaukat et al. [27] and Wang et al. [28] offered broad surveys on machine learning techniques and the specific challenges faced by smart grids. Lopez et al. [29] and Zakaria et al. [30] discussed current threats like malware and data breaches, categorizing machine learning models used in real-time threat detection. Joudaki et al.[31]developed into deep learning methods like CNNs and RNNs for securing the communication and power infrastructure. Mazhar et al. [32] and Burgos et al. [33] evaluated different supervised and unsupervised learning strategies for anomaly detection. Sahani et al. [34] focused on machine learning-based measures to safeguard data privacy and defend against advanced cyber threats such as phishing and insider attacks. Collectively, these studies highlight the critical role of AI in enhancing smart grid security and outline future research directions.

3.5 Smart Grid Cyber Security Incidents

Smart grid cybersecurity incidents are critical events that target the technological infrastructure of modern power grids, posing severe risks to both grid stability and national security. These incidents often exploit vulnerabilities in the complex and interconnected components of smart grids, including Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and Internet of Things (IoT) devices. Notable incidents, such as the 2015 Ukraine Power Grid cyber-attack, the Mirai botnet attack on IoT devices in 2016, and the 2020 Solar Winds supply chain attack, illustrate a shift towards more sophisticated and targeted assaults. These attacks disrupt operations, cause power outages, and potentially compromise sensitive data. Responses have evolved by incorporating advanced intrusion detection systems, machine-learning-based anomaly detection, and more stringent regulatory measures to enhance the resilience of smart grids against such threats. The timeline of Smart Grid Cyber security incidents along with the mapping of significant events and attacks over the years are mentioned in Table 2. The content of the table discusses cyber-attack sophistication and evolved responses for the smart grid.

Table 2. Time line of smart grid cyber security incidents

Year	Incident	Details	Impact	Response	Paper
2015	Ukraine Power Grid Cyber attack	Attackers remotely Accessed and disabled substations in Ukraine, causing Wide spread power outages.	Service Disruption for 225,000 people.	Heightened focus On securing control Systems and Advanced intrusion detection.	Cherepanov et. al, Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet. Retrieved From ESET Research.
2016	Mirai Botnet Attack	Mirai botnet Linked to Disruptions in Smart grids, Highlighting IoT vulnerabilities.	Large-scale service Interruptions and data breaches.	Adoption of stricter IoT security Protocols and Enhanced monitoring.	Dragos ,Inc., Ukraine Cyber-attacks: ICS Cyber Kill Chain Analysis. Retrieved From Dragos.
2017	Industroyer Malware	Industroyer malware Targeted industrial Control systems, Causing severe outages.	Severe service outages and potential Damage to infrastructure.	Introduction of Advanced threat detection Techniques using ML.	Cherepanov et.al, Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet. Retrieved From ESET Research.
2018	Attack on U.S. Power Utility	A cyber attack Targeted an U.S. utility, resulting In data breaches But no outages.	Concerns About data Integrity and Confidentiality.	Use of AI-driven Anomaly detection To monitor grid activity.	U.S. Cyber security & Infrastructure Security Agency (CISA). Colonial Pipeline Ransomware Attack Report. Retrieved from CISA.
2019	North American Electric Reliability Corporation	NERC issued a Cyber security advisory, Warning against state-sponsored Cyber-attacks.	Increased Awareness of critical infrastructure vulnerabilities.	Strengthened regulatory Compliance and updated Frame works.	North American Electric Reliability Corporation (NERC). Cyber security Advisory for Critical Infrastructure. Retrieved

	(NERC) Alert				from NERC.
2020	Solar Winds Supply Chain Attack	Solar Winds Software attack Affected utilities, Exposing grid data.	Global implications on grid management software security.	Focused on supply Chain security and Integrated ML Models for real-time monitoring.	Solar Winds. Solar Winds Supply Chain Attack Report Retrieved from Solar Winds.
2021	Colonial Pipeline Ransomware Attack	Ransomware Attack on The Colonial Pipeline highlighted the risks to interconnected grid systems.	Service Disruption and Panic buying Of fuel.	Strengthened Response plans and Use of predictive ML models for Ransomware patterns.	U.S. Cyber security & Infrastructure Security Agency (CISA). Colonial Pipeline Ransomware Attack Report Retrieved from CISA.
2023	Emerging IoT-based Attacks	Minor attacks Targeted IoT- Based devices, exploiting Vulnerabilities In edge components.	No major outages but data breaches and Slowdowns.	Increasing reliance On AI and ML-Based tools for Attack prediction And neutralization.	Mohamed M et.al, Emerging applications of IoT and cyber security for electrical power systems

4. PROPOSED SOLUTION IN SMART GRID COMMUNICATION ARCHETECTURE

Compatibility and interoperability challenges remain a significant concern in the smart grid environment owing to the diversity of devices and communication protocols. Smart grid networks consist of many components, ranging from basic low-power sensors to sophisticated high-performance processors. This heterogeneity makes seamless integration difficult and often leads to security vulnerabilities during the data aggregation processes, as highlighted in the IBM model [9]. For example, when different protocols interact, incompatibilities can create blind spots in the network, thereby exposing critical data to cyber threats.

To address these issues, this paper proposes a shift towards a unified, IPv6- based communication system. IPv6, when deployed over low-power wireless personal area networks (6LoWPAN) [25-26], offers the advantage of unique addressability and direct Internet connectivity for all smart grid components. This approach simplifies the communication architecture by eliminating the need for multilayer data aggregation, thereby reducing security risks and improving the overall system efficiency. Instead of relying on intermediary aggregation points, data can be transmitted directly to the application layer using standard IP-based protocols over Wi-Fi or 4G networks, as illustrated in the enhanced version of the smart grid architecture diagram. This solution leverages the vastly expanded address space of IPv6—capable of supporting 2^128 unique addresses—compared to the 4 billion addresses available under IPv4 (2^32). This capacity is critical for scaling IoT deployments within smart grids, ensuring that each device, from edge sensors to control systems, can be uniquely identified and managed securely.

The proposed model represents a Smart Electric Grid system that connects various devices and platforms through a cloud-based architecture using the World Wide Web (WWW), as shown in Figure 5. It integrates in-home devices, smart meters, substation/grid devices, and distributed energy resources with different layers of software and system management to enable efficient control and real-time data analysis. The key components of the proposed architecture are as follows:

1. **Device Layer:** This layer comprises different types of devices connected to the smart grid.
   - **In-home Devices (IP0, IP1, IP2):** Smart appliances, home automation systems, and energy management devices are some examples. These devices monitor and control electricity consumption at the consumer level.
   - **Smart Meter (IP3**): It acts as the central gateway between in-home devices and the rest of the grid. Measures electricity usage, supports two-way communication, and manages demand-response operations.
   - **Substation and Grid Devices (IP4 and IP5):** This includes intelligent sensors, voltage regulators, and automated switches located at substations or distribution lines. It facilitates grid reliability, real-time monitoring, and automated fault detection.
   - **Mobile Devices (IP6, IP7):** This comprises mobile control systems and field devices used by operators for remote management and data collection.
   - **Distributed Resources (IPn):** Distributed Energy Resources (DERs), such as solar panels, wind turbines, and battery storage units. It contributes to power generation, energy storage, and grid stabilization.
2. **System Integration Platforms:** The integration layer manages the interoperability and coordination between the different components of the smart grid.
   - **Computer Infrastructure:** Represents the hardware and network infrastructure that supports data storage, processing, and secure communication.
   - **System Management:** Software and control systems that handle grid operations, load balancing, resource optimization, and fault management.
   - **Application & Data Integration:** Middleware platform that aggregates data from various devices, standardizes formats, and enables seamless integration across multiple layers.
3. **Software Layers:** This segment deals with the interface and analytical tools for decision-making and user interactions:
   - **Presentation Layer:** User interfaces, graphical dashboards, and visualization tools for stakeholders to monitor the grid performance and health status.
   - **Apps and Analytics Layer:** This layer comprises applications and analytical tools for data-driven decision-making. This also supports functions such as predictive maintenance, demand forecasting, and optimization of energy resources.
4. **Connectivity Via The World Wide Web (Www)**
   - All the components were interconnected through the World Wide Web, highlighting a cloud-based architecture.
   - This connectivity enables real-time data exchange, remote monitoring, and control across the grid using secure Internet protocols.

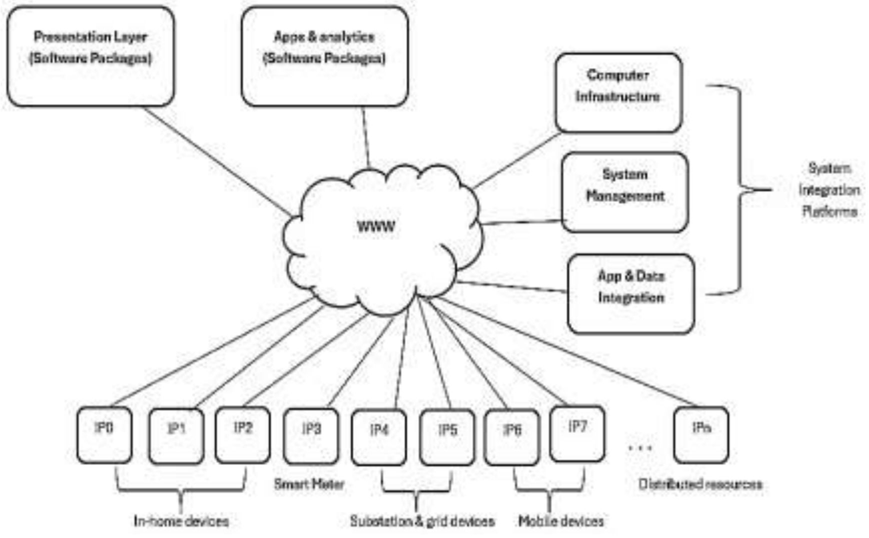

Figure 5. Proposed smart grid model

The proposed model integrates distributed devices, advanced system management platforms, and software layers to achieve a flexible, scalable, and intelligent electric grid system. Through this architecture, real-time monitoring, efficient resource management, and proactive maintenance are achieved, enhancing the overall grid stability and reliability.

5. CONCLUSION

The rapid evolution of smart grids has introduced unprecedented opportunities and significant cybersecurity challenges. As smart grid systems incorporate more interconnected devices, including sensors, smart meters, and IoT components, the attack surface expands, rendering traditional security measures insufficient. This review examines various machine learning models and approaches that have been employed to address these challenges, focusing on enhancing the detection and mitigation of cyber threats. The analysis highlights that while machine learning and artificial intelligence are promising tools for developing robust security frameworks, there are still critical gaps in compatibility, data aggregation security, and protocol standardization.

To overcome these challenges, this paper proposes transitioning to a unified IPv6-based communication layer, which simplifies data exchange, reduces security risks, and allows for the direct connectivity of all devices. This approach, along with the integration of advanced security protocols such as IP sec, can enhance the real-time detection and response capabilities of smart grid systems, making them more resilient to cyber-attacks. Future research should focus on refining these models to address merging threats, ensuring scalability, and creating comprehensive solutions that account for both edge device security and system-wide protection. By aligning research efforts with these goals, it is possible to build a more secure and reliable smart grid infrastructure capable of withstanding sophisticated cyber threats.

REFERENCES

[1]. NIST, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

[2]. R. Apel,"Smart Grid Architecture Model: Methodology and Practical Application," in Workshop of Electrical Power Control Centers, 2013.

[3]. H. Brown, S. Suryanarayanan, S. Natarajan, and S. Rajopadhye, “Improving Reliability of Islanded Distribution Systems with Distributed Renewable Energy Resources,” IEEE Trans. on Smart Grid, 3(4), pp. 2028–2038, 2012.

[4]. M. Miller, M. Johns , E. Sortomme, and S.Venkata,S. “Advanced integration of distributed energy resources” in Power and Energy Society General Meeting, pp. 1-2, July 2012.

[5]. R. Morales Gonzalez, B.A sare- Bediako, J. Cobben, W.Kling , G. Scharrenberg, and D. Dijkstra, “Distributed energy resources for a zero-energy neighborhood,” in 3rd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, pp.1-8, 2012.

[6]. W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, 57(7), pp. 1344-1371, 2013.

[7]. W. Wang, "A survey on the communication architectures in smart grids," Computer Networks,vol. 55, no. 15, pp. 3604-3629, 2011.

[8]. G. F. Reed, P. A. Philip, A. Barchowsky and C. J. Lippert, "Sample survey of smart grid approaches and technology gap analysis," in Innovative Smart Grid Technologies Conference Europe, 2010.

[9]. G. Garner, "Designing Last Mile Communications Infrastructures for Intelligent Utility Networks (Smart Grid)," IBM Intelligent Utility Network (IUN) Communication Services, 2010.

[10]. Claudio Lima, "An Architecture for the Smart Grid,” in IEEE P2030 Smart Grid Comm. Architecture SG1 ETSI Workshop, pp. 1-27, 2011.

[11]. H. Naidua and K. Thanushkodib, “Recent Trends in SCADA Power Distribution Automation Systems,” in Bangladesh Journal of Scientific and Industrial Research, 45(3), pp. 205-218, 2010.

[12]. A.Rezai,P.Keshavarzi,andZ.Moravej,“Secure SCADA communication by using a modified key management scheme,” ISA Transactions, 52(4), pp. 517-524, July 2013.

[13]. E. Knapp and R.Samani,“Security Models for SCADA ,ICS,and Smart Grid,” in Applied Cyber Security and the Smart Grid, ch. 5, 2013.

[14]. M. B. Line, I. A. Tondel and M. G. Jaatun, "Cyber security challenges in Smart Grids," in 2nd IEEE PES International Conference and Exhibition, Innovative Smart Grid Technologies (ISGT Europe), Manchester, 2011.

[15]. H. Khurana, M.Hadley, L.Ningand D.A. Frincke,"Smart grid security issues," IEEE Security & Privacy, 7(1), pp. 81-85, 2010.

[16]. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3, Nat'l Institute of Standards and Technology, 2014.

[17]. J.-H.Jun,D.Lee,C.-W.AhnandS.-H.Kim," DDoS Attack Detection Using Flow Entropy and Packet Sampling on Huge Networks," in the13th International Conference on Networks,Nice,2014.

[18]. G. Meng and N. Wang, "A Network Intrusion Detection Method Based on Improved K-Means Algorithm," Advanced Science and Technology Letters, 53(1), pp. 429-433, 2014.

[19]. S. Shin, S. Lee, H. Kim and S. Kim, "Advanced probabilistic approach for network intrusion forecasting and detection," Expert Systems with Applications, 40(1), pp. 315-322, 2013.

[20]. D. Lin, "Network Intrusion Detection and Mitigation against Denial-of-Service Attack," WPE- II Report, Univ. of Pennsylvania, Apr. 2013.

[21]. W. Xu, W. Trappe, Y. Zhang and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," in 6th ACM Int'l Symposium on Mobile Ad Hoc Networking and Computing, 2005.

[22]. C. Popper, M. Strasser and S. Capkun, "Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques," IEEEJ. on Selected Areasin Comm., 28(5),pp. 703- 715, 2010.

[23]. E.K.Lee, M.GerlaandS.Y.Oh," Physical Layer Security in Wireless Smart grid," IEEE Comm. Magazine, 50(8), pp. 46-52, 2012.

[24]. M. Kammerstetter, "Architecture-Driven SMART GRID Security Management," in ACM Workshop on Information Hiding and Multimedia Security, 2014.

[25]. V. Gungor, D.Sahin,T.Kocak, S.Ergut, C. Buccella, C. Cecati,and G. Hancke, "A Survey on Smart Grid Potential Applications and Communication Requirements," IEEE Trans. on Industrial Informatics, 9(1), pp. 28-42, 2013.

[26]. Z. HuangandF. Yuan, "Implementation of 6LoWPAN and Its Application in Smart Lighting," Journal of Computer and Communications, vol. 3, pp. 80-85, 2015.

[27]. Shaukat,Kamran&Luo,Suhuai&Varadharajan,Vijay&Hameed,Ibrahim&Xu,Min., " A Survey on Machine Learning Techniques for Cyber Security in the Last Decade", IEEE Access. 10.1109/ACCESS.2020.3041951.

[28]. Wang, Wenye & Lu, Zhuo, "Cyber security in the Smart Grid: Survey and challenges. Computer Networks", 57. 1344–1371. 10.1016/j.comnet.2012.12.017.

[29]. Lopez, Carlos & Sargolzaei, Arman & Santana, Hugo & Huerta, Carlos, "Smart Grid Cyber Security: An Overview of Threats and Countermeasures", Journal of Energy and Power Engineering. 9. 10.17265/1934-8975/2015.07.005.

[30]. Zakaria El Mrabet,Naima Kaa bouch, Hassan ElGhazi, Hamid ElGhazi, "Cyber-security in smart grid: Survey and challenges", Computers & Electrical Engineering, Volume 67,2018,Pages469-482, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2018.01.015.

[31]. M. Joudaki, P. T. Zadeh, H. R. Olfati and S. Deris, "A Survey on Deep Learning Methods for Security and Privacy in Smart Grid," 2020 15th International Conference on Protection and Automation of Power Systems (IPAPS), Shiraz, Iran, 2020, pp. 153-159, doi: 10.1109/IPAPS52181.2020.9375569.

[32]. Mazhar, T.; Irfan, H.M.; Khan, S.; Haq, I.; Ullah, I.; Iqbal, M.; Hamam, H., "Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Block chain Methods", Future Internet 2023, 15, 83. https://doi.org/10.3390/fi15020083.

[33]. Guato Burgos, M.F.; Morato, J.; Vizcaino Imacaña, F.P., "A Review of Smart Grid Anomaly Detection Approaches On Artificial Intelligence", Appl.Sci.2024,14,1194. https://doi.org/10.3390/app14031194.

[34]. Sahani,N.,Zhu,R.,Cho,J.H.,&Liu,C.C.(2023), " Machine learning-based intrusion detection for smart grid computing: A survey", ACM Transactions on Cyber-Physical Systems, 7(2), 1-31.

[35]. Chere panov, A., Lipovsky, R., & ESET Research, " Industroyer: Biggest Threat to Industrial Control Systems Since Stuxnet", Retrieved from ESET Research.

[36]. Dragos, Inc., "Ukraine Cyber attacks: ICS Cyber Kill Chain Analysis", Retrieved from Dragos.

[37]. North American Electric Reliability Corporation (NERC), "Cyber security Advisory for Critical Infrastructure" Retrieved from NERC.

[38]. Solar Winds.(2020), "Solar Winds Supply Chain Attack Report", Retrieved from Solar Winds.

[39]. U.S.Cyber security & Infrastructure Security Agency (CISA) (2021) "Colonial Pipeline Ransomware Attack Report", Retrieved from CISA.

[40]. Mohamed M., Mahmoud Elsisi, Mostafa M. Fouda, Diaa-Eldin A. Mansour, Matti Lehtonen, "Emerging applications of IoT and cyber security for electrical power systems", 2023, IET Generation, Transmission & Distribution published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology, vol.no.17, pp. 4453–4456, doi: 10.1049/gtd2.13012.