

A Multi-Layer Conceptual Security Architecture Toward Robust and Resilient SDN-Enabled Smart Grids

Seref Sağiroğlu^{*†}, Mehmet Demirci^{*}, Yılmaz Atay^{*}, Murat Dener^{**}, M. Sedef Demirci^{*},
Ali Kara^{***}, Samed Al^{**}, Selcuk Yılmaz^{**}

^{*} Department of Computer Engineering, Faculty of Engineering, Gazi University, Ankara, Türkiye

^{**} Department of Information Security Engineering, Graduate School of Natural and Applied Sciences, Gazi University, Ankara, Türkiye

^{***} Department of Electrical and Electronics Engineering, Faculty of Engineering, Gazi University, Ankara, Türkiye

{ss, mdemirci, yilmazatay, muratdener, sedefgunduz, akara, samedal, selcuk.yilmaz1}@gazi.edu.tr

[†] Corresponding Author; Seref Sagiroglu, Department of Computer Engineering, Faculty of Engineering, Gazi University, Ankara, Türkiye, Tel: +90 312 582 3124, Email: ss@gazi.edu.tr

Received:01.02.2026 Accepted:07.06.2026

Abstract- Smart grids integrate advanced communication and control technologies to improve the efficiency and reliability of power delivery, but their interconnected and heterogeneous nature expands the attack surface. Recent attacks ranging from malware to false data injection have demonstrated the need for robust, layered defenses spanning physical devices, network infrastructure, control systems, and applications. Software-defined networking (SDN) offers centralized, programmable control over grid communications to dynamically isolate threats and reroute traffic during attacks. Securing SDN-enabled smart grids requires a defense-in-depth approach that combines diverse emerging technologies. This paper proposes a multi-layer conceptual security architecture leveraging blockchain for data integrity, explainable AI for transparent decision-making, generative AI for adaptive threat detection, quantum-safe cryptography for future resilience, big data analytics for anomaly detection, and radio frequency fingerprinting for device authentication. We present our model and discuss how each component contributes to a cohesive security architecture. We also identify open research challenges for integrating these solutions seamlessly to move toward more secure grids in the future.

Keywords Software-defined networking (SDN), cybersecurity, smart grid, generative AI, radio frequency fingerprinting

1. Introduction

A smart grid (SG) is an advanced electrical network that enables the bidirectional flow of both electricity and data between power generation facilities and end users through modern communication technologies [1]. The SG infrastructure consists of two fundamental layers: the power

system layer and the communication layer. The power system layer encompasses key operations such as electricity generation, transmission, and distribution. Meanwhile, the communication layer serves as the backbone that enables seamless information exchange between these power system components [2].

Traditional smart grid communication networks typically rely on legacy technologies like Multiprotocol Label Switching (MPLS). However, these conventional approaches are not fully aligned with the dynamic nature of SGs. One major limitation is their static architecture—whenever a new service needs to be integrated, the network components must be manually reconfigured. This lack of adaptability makes expansion and innovation within the grid challenging. Additionally, since different energy providers manage and operate their own networking equipment, the infrastructure becomes increasingly fragmented as more vendors enter the market. This heterogeneity leads to interoperability issues, network inefficiencies, and an increased risk of service disruptions. Moreover, the fragmented architecture creates security vulnerabilities, making the grid susceptible to cyber threats [3].

Software-Defined Networking (SDN) emerges as a promising solution to these challenges by transforming the communication layer into a programmable network. It decouples network control from data forwarding devices, centralizing management through a software-based controller. This approach allows networks to be dynamically programmed and adapted to changing requirements [4]. With SDN, the grid can dynamically adjust to changes, optimize data flow, and enhance security, ultimately ensuring a more resilient and efficient SG communication framework. Fig. 1 illustrates how SDN is integrated into the communication infrastructure of the SG.

The architecture consists of three layers: data plane, control plane, and application plane. The data plane comprises grid components such as smart meters, sensors, and power management units (PMUs), as well as programmable networking hardware that forwards grid traffic based on instructions from the control plane [5]. The control plane is responsible for network intelligence and decision-making. It consists of one or multiple SDN controllers that establish traffic paths and forwarding rules, which are then programmed into SDN switches located in the data plane. The communication between the control and data planes is facilitated through the Southbound API, with OpenFlow being a common protocol for this purpose. This ensures secure message exchange between the control and data layers. At the highest level, the application plane hosts both smart grid and SDN-specific applications that perform key functions such as device management, voltage and frequency control, grid status monitoring, load balancing, traffic filtering, intrusion detection/prevention, and deep packet inspection. Through the Northbound API, applications dictate their policies to the controller, which then translates them into enforceable rules for SDN switches within the data plane [1].

Although SDN can enhance the security of smart grid architectures, its open nature introduces new security challenges for software-defined smart grid systems. In this paper, we propose a multi-layer security concept model for SDN-enabled smart grids. The rest of the paper is organized as follows: Section II describes our proposed multi-layer security concept model for SDN-enabled smart grids. Section III highlights open issues and future research directions in

the field. Section IV provides a discussion of all new concepts for smart grids. Finally, Section V summarizes the paper and gives concluding remarks.

2. Proposed Multi-Layer Security Concept Model

A security framework for SDN-enabled smart grids must incorporate solutions at multiple layers within the network to be effective and comprehensive. To this end, we propose a multi-layer security concept model that addresses threats at each layer of the system architecture, as illustrated in Fig. 2.

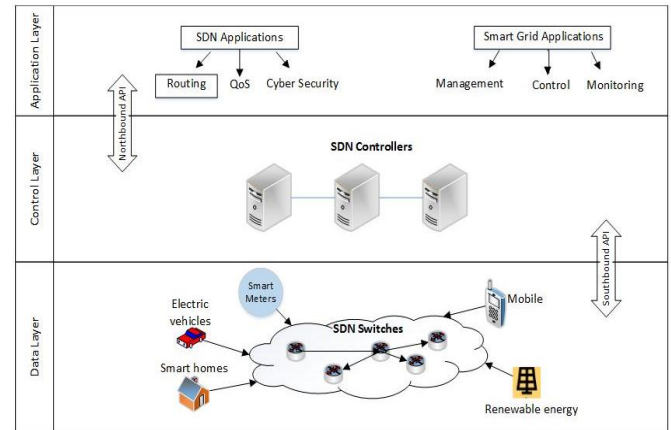


Fig. 1. Software-defined smart grid architecture (adapted from [1] and [6]).

The novelty of our framework can be explained in the following way:

- It incorporates security measures deployed at different layers to support defence in depth.
- It integrates SDN and NFV as central parts of the architecture.
- It focuses on emerging techniques such as radio frequency fingerprinting in the physical layer, which is often overlooked in existing proposals.

In this layered model, the smart grid's infrastructure is divided into the Physical/Perception layer, Network/Communication layer, Control layer, Application and Management layer for security governance. Each layer is secured using appropriate mechanisms, and cross-layer communication ensures that intelligence is shared between layers. This design follows the principle of defense in depth: even if an attacker penetrates one layer, additional layers of defense can contain the damage and protect grid functions.

Our proposed model should not be interpreted as a collection of independent security mechanisms, but as an integrated security architecture in which information and control flow continuously across layers. Security events detected at the Physical/Perception layer, such as the identification of a rogue device through radio frequency fingerprinting, are propagated to the Network/Communication layer, where the SDN controller can immediately update forwarding rules to isolate the affected device or redirect its traffic through additional security functions. Similarly, anomalies identified by

network monitoring or intrusion detection systems are communicated to the Control layer, allowing the controller to adapt routing policies, activate redundant communication paths, or deploy virtualized security services through NFV. At the Application and Management layer, information collected from all lower layers is aggregated by SIEM and analytics platforms, where AI-assisted correlation, blockchain-supported integrity verification, and risk assessment provide a comprehensive view of the system and generate coordinated response actions that are enforced throughout the architecture.

The proposed model therefore emphasizes orchestration rather than simply stacking security technologies. SDN serves as the central coordination mechanism that enables dynamic enforcement of security policies across all layers, while each emerging technology contributes a complementary capability. Radio frequency fingerprinting strengthens device identity assurance at the edge, blockchain provides integrity and traceability for critical operations, explainable and generative AI enhance intelligent detection and decision support, privacy-preserving analytics protect sensitive information, and quantum-safe cryptography prepares the communication infrastructure for future threats. By explicitly defining both the functional responsibilities of each layer and the interactions among them, the proposed model establishes a cohesive defense-in-depth architecture capable of adapting to evolving cyber threats while maintaining the operational requirements of smart grids. Each layer in our framework is further explained in the sections below.

2.1. Physical/Perception Layer

This layer includes field devices such as smart meters, sensors (e.g., PMUs), actuators, and intelligent electronic devices (IEDs) in substations. Securing the physical layer is crucial, as a compromised device can feed false data or disrupt grid operations at the source. Our model incorporates tamper-resistant hardware and physical security controls (like secure device enclosures and access restrictions) to reduce the risk of tampering. We also use device authentication mechanisms at this layer, including cryptographic authentication of device identities as well as emerging techniques like radio-frequency fingerprinting (RFF) as detailed in Sec. 3.8. Radio-based smart meters (sensors at the lowest level) transmitting data in real time is very typical. However, this may become challenging from a security perspective as rogue devices may be present. This could be adequately addressed in the physical layer with RFF, as illustrated in Fig. 3.

This configuration guarantees that all transmissions from the smart meters pass through the physical security barrier, i.e., RFF system, before reaching the upper layer systems. At the physical layer of smart grids, the star-of-stars network topology would be considered, which utilizes the fact that the data of all the sensors is concentrated at the relevant gateways. In this way, the RFF system hosted by the IoT gateways would serve as a barrier to not allowing readings from non-legitimate sources. Simply, it filters the rogue ones on a per-packet basis. By verifying that each sensor/actuator

is legitimate and behaving as expected, the system can detect impostor or rogue devices injecting malicious signals. Moreover, lightweight anomaly detection agents can also run on local controllers, using machine learning to flag abnormal control actions or measurements at the source. These measures ensure that the data entering the grid from the physical layer is trustworthy, forming the first line of defense against attacks such as sensor spoofing, false data injection, and device impersonation.

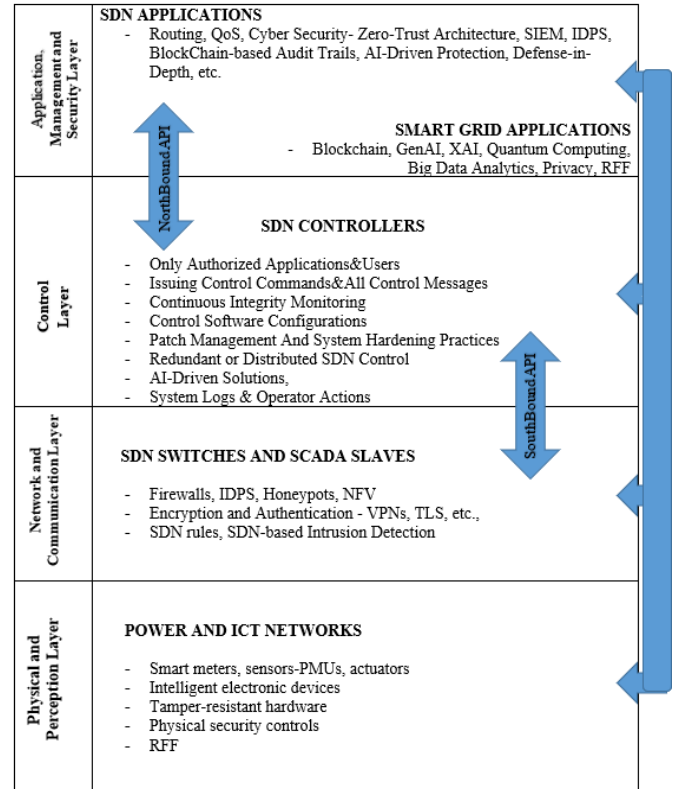


Fig. 2. A conceptual multi-layer security architecture for an SDN-enabled smart grid model (adapted from [1]-[5]).

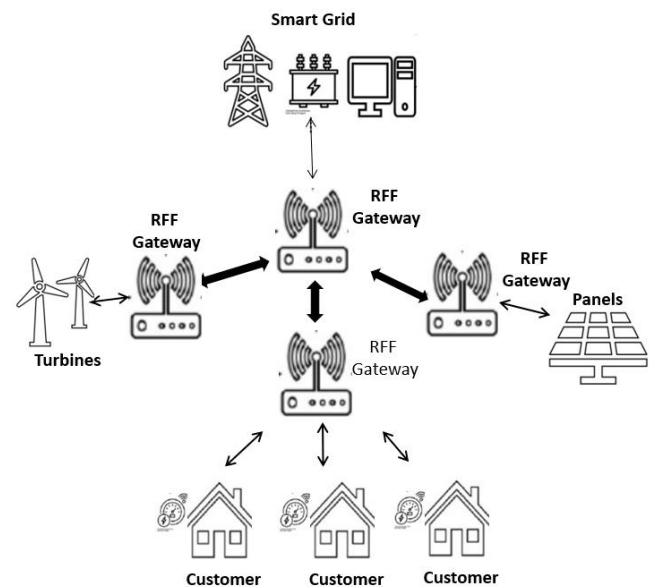


Fig. 3. Illustration of conceptual physical layer security (RFF) architecture for smart grid.

2.2. Network/Communication Layer

This layer comprises the communication links (wired or wireless) and networking hardware that connect grid devices and control centers. Here, the SDN controller plays a pivotal security role. All grid data traffic flows through SDN-enabled switches, which enforce network-wide security policies. Programmable switches are increasingly employed to improve flexibility, agility, and security [7, 8]. For instance, P4 switches can be leveraged to implement efficient defense against SYN flood attacks [9].

Our model uses the SDN controller to implement traffic whitelisting and segmentation, so that each device or subsystem only communicates with authorized endpoints. For example, a smart meter's data packets are only allowed to reach the metering database and not directly other meters, limiting lateral movement for an attacker. The controller also monitors traffic patterns for anomalies (e.g., sudden spikes that could indicate a DoS attack) and can dynamically reroute or block flows as needed. Communication links are secured with encryption and authentication (VPNs, TLS, etc.) to prevent eavesdropping and man-in-the-middle attacks. By segmenting and closely monitoring network traffic, the model contains malware propagation and mitigates threats like DDoS or routing attacks. If a substation network is compromised, SDN rules can isolate it from the rest of the grid while alternate paths maintain overall grid communication. This layered defense was demonstrated in the EU SDN-microSENSE project, which defined an SDN-based intrusion detection and self-healing framework to react to cyberattacks in real time. In essence, the network layer acts as the nerve center for detection and response, leveraging SDN's global view to enforce security across the grid [10].

2.3. Control Layer

The control layer refers to the central control systems and SDN controllers that manage grid operations. This includes SCADA master stations, distributed energy resource management systems, and the SDN controller itself (which links the communication network with grid applications). The SDN controller is also responsible for routing grid traffic through the security functions residing in the application plane. The decisions here can be optimized for minimizing link usage or energy consumption while preserving all security constraints. In order to do this, the controller software takes the topology of the SG communication network, the grid traffic matrix, along with their required security functions list that they must pass through, and a set of security function specifications as inputs. Then, it calculates paths for the flows and writes the calculated routing rules to the flow tables of the SDN switches. In this way, SG traffic can be steered through the desired points (e.g., trust nodes) if needed for in-path monitoring and security actions such as blocking, rate limiting, rerouting, etc. can be applied. Alternatively, if trust nodes are virtualized, they can be deployed dynamically at chosen locations. Placing these virtual trust nodes closer to the edge

could be preferable for reduced latency, which is a common goal for most real-world SG deployments.

Securing the control plane is paramount because an attack here can potentially override grid commands or blind the operators to ongoing events. Our model ensures the integrity and availability of control layer components through several measures. First, strict access control and authentication are enforced for any interaction with the SDN controller or SCADA systems – only authorized applications and users can issue control commands, and all control messages are cryptographically signed to prevent forgery. Second, we incorporate continuous integrity monitoring for control software, using cryptographic checksums and anomaly detection on controller behavior (e.g., alert if the controller begins installing unexpected flow rules that deviate from its normal patterns). Third, robust patch management and system hardening practices are applied: keeping the controller and servers updated against known vulnerabilities, disabling unnecessary services, and running them in secure, isolated environments. Moreover, the model supports redundant or distributed SDN control: multiple synchronized controllers can take over if one fails or is compromised, significantly reducing the risk of a single point of failure. To detect sophisticated threats like stealthy malware or insider misuse, we utilize AI-driven solutions that analyse system logs and operator actions for anomalies (e.g., unusual sequence of commands at odd hours). In this way, our multi-layer model defends against attacks trying to hijack the grid's decision-making processes, such as false command injection, controller exploits, or timing manipulation attacks.

2.4. Application Management and Security Layer

The application layer encompasses the end-user services and grid management applications such as energy management systems, demand response programs, distributed energy resource (DER) trading platforms, and data analytics dashboards. It also includes databases storing smart meter data and other business systems. Furthermore, network security applications are integrated as virtualized functions in this layer, such as firewalls, intrusion detection/prevention systems (IDPS), and honeypots, which can be deployed on demand at strategic points via network function virtualization (NFV). The proposed framework is modular and extensible: New security functions can be added and updated independently as needed. In this way, shortcomings with regard to the security mechanisms can be addressed without the need to change the other layers or the general architecture.

Our model employs role-based access control and multi-factor authentication to ensure that only legitimate users and software services can access sensitive smart grid data or control functions. All transactions (e.g., energy trading records, meter reading updates) are logged on an immutable ledger to provide tamper-evident records of grid operations. This helps in post-incident forensics and in real-time detection of unauthorized changes. Big data analytics are heavily utilized in this layer to make sense of the massive volumes of grid data for both operational efficiency and

security insights. In our model, we integrate such analytic engines with an emphasis on explainability so that grid operators can validate and respond appropriately. We also embed privacy-preserving techniques in applications that handle customer data, ensuring compliance with regulations and protecting consumers. Our model also supports situational awareness dashboards that unify security information from all layers. By hardening applications and safeguarding data, the multi-layer model mitigates threats such as database breaches, phishing and social engineering, and data manipulation attempts.

Cutting across all the above layers is a dedicated management layer responsible for orchestrating security policies and responses – essentially the security brain of the architecture. This layer comprises components such as a Security Information and Event Management (SIEM) system, threat intelligence feeds, and the risk assessment and self-healing frameworks. It implements a holistic Zero-Trust Architecture (ZTA) throughout the grid. ZTA continuously verifies each user, device, and application action, rather than assuming any implicit trust based on network location. For example, even an internal control center user must re-authenticate and is only granted least-privilege access. The management layer also runs continuous risk assessments, evaluating the cybersecurity posture of grid assets in real time. If a high risk is identified for certain assets, the system can proactively adjust the controls. Correlation engines in this layer aggregate alerts from across the network using AI to recognize complex multi-stage attacks. Upon detecting a credible threat, the management layer can trigger the self-healing mechanisms: for instance, instructing the SDN controller to quarantine malicious traffic, re-configuring grid topology to maintain stability, or activating backup systems. By overseeing and unifying the defense strategy, the management layer ensures that the multi-layer defenses work in concert rather than in isolation and implements policies that span multiple layers.

Overall, the proposed multi-layer model creates a comprehensive security shield around the SDN-enabled smart grid. In the next section, we summarize how key security technologies are mapped onto this layered architecture, highlighting their benefits and challenges.

3. Open Research Challenges and Future Directions

This section examines the potential of technologies such as blockchain-based secure data sharing, big data analytics, quantum computing-enhanced encryption, XAI-driven transparent decision-making, and Generative Artificial Intelligence-enabled innovative data modeling in SDN-enabled smart grids.

3.1. Blockchain

In our multi-layer model, blockchain can serve as a distributed, tamper-proof ledger for recording events and transactions across the grid. For example, power generation data, grid control commands, and energy trading between prosumers can be logged in a blockchain to ensure transparency and integrity. Blockchain also introduces decentralization: critical security functions such as

authentication or key management can be distributed among many nodes, reducing single-point-of-failure risks. Microgrid deployments have embraced blockchain for local energy trading to provide a secure and transparent platform for tracking energy transactions between homes or DER units. This decentralization aligns well with smart grid trends toward distributed generation and storage, enabling trust in transactions of power or data between entities that may not fully trust each other [11–13].

Recent studies have shown that blockchain can be integrated with SDN-based smart grids, cyber-physical systems (CPS), and IoT communication infrastructures to secure both control and data planes. In particular, blockchain has been used to maintain immutable records of SDN flow rules, ensuring consistency among distributed controllers and enabling version control of network policies [14,15]. By comparing hash values of flow tables stored on-chain with those deployed in switches, compromised or rogue network elements can be detected and isolated [16]. Furthermore, blockchain has been exploited to support collaborative intrusion detection and trustworthy data sharing in SDN-enabled CPS environments. Experiments show that such blockchain-assisted cooperative IDS frameworks achieve higher robustness and detection performance compared to conventional approaches [17].

Blockchain-supported SDN frameworks have also been applied to peer-to-peer energy trading and vehicle-to-grid (V2G) scenarios, where transactions are validated in a decentralized manner, thereby reducing latency and network overhead while preventing fraudulent trades and improving trust among participating entities [18, 19]. In addition, blockchain-based SDN communication architectures have been proposed to protect inter-controller communication and to guarantee secure dissemination of control messages across distributed smart grid domains [20].

Integrating blockchain into smart grids faces research challenges, primarily regarding scalability and performance: current public blockchain networks struggle with high throughput and low latency requirements. Processing all events generated by a national-scale smart grid in a blockchain could introduce delays that are unacceptable for real-time grid control. Solutions such as permissioned blockchains operating among grid stakeholders with more efficient consensus mechanisms (e.g., Proof-of-Authority or Practical Byzantine Fault Tolerance) are being explored to improve throughput [14, 16, 17, 19]. Another challenge is the energy and resource cost of blockchain mechanisms. Some consensus algorithms (e.g., Proof-of-Work) are too computationally intensive for the energy efficiency goals of smart grids. Moreover, data privacy on blockchains remains an open issue and techniques such as on-chain hashing with off-chain storage, blockchain-based access control, and privacy-preserving ledgers are proposed to reconcile transparency with confidentiality [17, 19, 20]. Therefore, further research is required to design lightweight consensus mechanisms and hierarchical or edge-assisted blockchain architectures that can meet the stringent performance requirements of future smart grids.

3.2. Explainable AI (XAI)

Artificial intelligence (AI) and machine learning (ML) are increasingly being used in smart grids for applications like load forecasting, fault detection, and cybersecurity. However, most AI models – especially powerful ones like deep learning (DL) – operate as “black boxes” that do not readily explain why they made a certain decision or prediction. In a critical infrastructure like the power grid, this lack of transparency is problematic. XAI addresses this challenge by providing techniques that make AI decisions more interpretable to humans. For smart grid security, XAI is crucial because it can bridge the gap between complex AI-driven defenses and the operators who oversee the grid by providing insights that allow a human operator to verify an alert and to understand the nature of the threat. It also helps in compliance and governance – regulators may require utilities to provide reasoning for automated decisions that affect customers. From a technical perspective, XAI can identify biases or blind spots in AI models by revealing their focus.

The challenge is that achieving explainability often comes at a cost. Simpler ML models are more interpretable but may not capture the complexity of grid data as well as DL models. Conversely, advanced models can achieve high accuracy but are intrinsically hard to interpret. In a smart grid, another difficulty is the scale and interdependency of the data – an AI’s decision might be influenced by hundreds of input points, making comprehensive explanation a non-trivial task. XAI should produce concise real-time insights to help accelerate the adoption of sophisticated ML in smart grid operations. Moving forward, collaboration between AI researchers and power engineers is essential to develop XAI tools tailored for the grid’s needs, potentially setting industry standards on how AI decisions in smart grids should be documented and audited.

3.3. Generative AI

Generative Artificial Intelligence (GenAI), particularly Large Language Models (LLMs) and Generative Adversarial Networks (GANs), has rapidly advanced in recent years and introduces both promising capabilities and unresolved challenges for smart grid cybersecurity. Generative AI refers to models that can create new data instances resembling their training data, enabling them to generalize beyond fixed patterns and adapt to evolving conditions. In the context of SDN-enabled smart grids, where communication flows, control logic, and attack surfaces are highly dynamic, such adaptability is especially attractive. One key security application of generative AI is the enhanced detection of novel or evolving cyber threats. LLMs can be fine-tuned to analyse heterogeneous data sources, including SDN controller logs, network traffic flows, SCADA events, and operational measurements, to identify suspicious behavior or infer coordinated attack patterns. Unlike traditional machine learning models that often require retraining when attackers change tactics, LLMs may generalize from broader contextual knowledge to flag unusual correlations or deviations from normal operational behavior [21, 22].

Beyond automated detection, generative AI enables natural language interaction between human operators and security systems. An LLM-based assistant could allow grid operators to pose high-level queries, such as whether there are indications of coordinated attacks on substation automation systems within a specific time window, and receive synthesized responses supported by relevant evidence extracted from logs and telemetry. Such capabilities may improve situational awareness and decision support, particularly during complex multi-stage attacks, while reducing the cognitive burden on human operators [23]. In addition, generative models can be leveraged for realistic synthetic data generation. GANs can produce simulated cyber-attack traffic, anomalous grid measurements, or false data injection scenarios that are difficult or risky to obtain from real-world smart grid deployments. These synthetic datasets can be used to train and evaluate intrusion detection and anomaly detection systems under a wider range of adversarial conditions, thereby improving robustness and generalization [24, 25].

Despite these potential benefits, the integration of generative AI into smart grid security architectures raises several open research challenges. A fundamental concern is the reliability and trustworthiness of LLM outputs. Generative models are often characterized as black boxes and may hallucinate plausible but incorrect information if insufficiently constrained or queried outside their effective knowledge domain. In a safety-critical environment such as a smart grid, fabricated alerts, inaccurate explanations, or misleading recommendations could lead to false alarms, unnecessary control actions, or delayed responses to genuine attacks [26]. Addressing this issue requires further research into constrained generation, uncertainty estimation, explainability mechanisms, and human-in-the-loop validation strategies.

Another unresolved issue is the computational and architectural feasibility of deploying generative models in smart grids. Large-scale LLMs typically require significant computational resources and may be impractical for continuous, real-time analysis at the grid edge or within substations. Running such models centrally may also introduce latency and single points of failure. Research into model distillation, quantization, hierarchical edge–fog–cloud deployment strategies, and event-driven or on-demand use of generative AI is necessary to balance performance, scalability, and resilience [27].

Finally, generative AI itself introduces new attack vectors. Adversaries may attempt to manipulate model behavior through data poisoning, adversarial prompts, or prompt injection attacks, potentially influencing security decisions or obscuring malicious activity. Understanding the robustness of generative AI under adversarial conditions and developing defenses against AI-specific attacks remain open research problems, particularly in the context of critical infrastructure protection [28].

3.4. Privacy

Preserving privacy in smart grid environments remains a significant open research challenge due to the inherently

heterogeneous nature of grid infrastructures and the widespread deployment of low-power, resource-constrained devices. Smart grids continuously collect and transmit large volumes of fine-grained data, including consumption patterns, device status, and operational telemetry, much of which may be considered sensitive or personally identifiable. Implementing comprehensive privacy-preserving frameworks, such as consent management mechanisms, encryption of personal data, access control policies, and data minimization strategies, inevitably increases system complexity and may introduce additional computational, communication, and latency overhead. These trade-offs are particularly problematic in time-critical grid operations, where delays or performance degradation can negatively impact stability and reliability.

Big data security analytics further complicates the privacy landscape. While large-scale data aggregation is essential for detecting anomalies, coordinated attacks, or long-term trends, indiscriminate collection and centralized analysis of raw data can raise serious privacy and regulatory concerns. Without appropriate safeguards, such practices may be perceived as overly intrusive by consumers or may conflict with data protection regulations, leading to public resistance or regulatory intervention. Consequently, security analytics must be designed to operate on aggregated and anonymized data whenever possible, or to ensure that explicit and transparent consent mechanisms are in place. Balancing the need for detailed security visibility with privacy preservation remains a non-trivial design challenge in smart grid architectures.

Federated learning has emerged as a promising and cost-effective approach to addressing these concerns. By enabling machine learning models to be trained locally on edge devices or regional nodes, federated learning minimizes the need to transmit raw data to centralized processing facilities. Instead, only model updates or gradients are shared, significantly reducing the risk of sensitive data exposure while also lowering network load and communication latency. This decentralized learning paradigm aligns well with the distributed nature of smart grids and supports scalability across large numbers of heterogeneous devices [1, 29]. However, deploying federated learning in smart grid security contexts introduces its own open issues. Challenges include handling non-independent and non-identically distributed (non-IID) data across devices, ensuring robustness against compromised or malicious participants, and managing the additional coordination and synchronization overhead required for model aggregation. Machine learning models that prioritize local learning and minimize data sharing can achieve a more favorable balance between security effectiveness, privacy preservation, and system performance. Therefore, prioritizing federated learning-based approaches in the development of security solutions is well aligned with the requirements of a secure, privacy-conscious smart grid platform [1, 29, 30].

3.5. Adversarial AI

Many common security applications rely on machine learning models, which can be directly targeted by adversarial attacks. The ability of a model to maintain good

performance under adversarial attacks is called adversarial robustness [31]. While there are emerging solutions to improve the robustness of ML models, this is still a fairly nascent area and new attack methods are also being proposed to cripple naïve models. In recent years, researchers have proposed various methods to improve the robustness of ML-based IDPSs and other security systems [32, 33]. The proposed framework incorporates robust IDPS models from recent literature. Metrics and methodologies used in robustness evaluation must be determined and applied to any security solution at this layer before its deployment.

Poisoning attacks are generally considered highly dangerous because they compromise the fundamental decision-making process of ML models. A modern smart grid contains several points where careful injection of fake or falsely labeled data can cause crucial issues such as inaccurate forecasting, weakened anomaly detection, and wasteful or insufficient planning [34]. The adverse effects of poisoning attacks may linger for months after the contamination of the training data, and in the case of repeated poisoning, persistent unreliability and inefficiency become the norm for the grid. Best practices must be applied to combat poisoning, including the validation and sanitization of training data, and continuous monitoring of model inputs and outputs to detect concept drift before it leads to the normalization of subpar or dangerous operating conditions [35].

3.6. Quantum-Safe Security

Quantum computing poses a fundamental threat to existing cryptographic mechanisms used in smart grids, as quantum algorithms such as Shor's algorithm will be able to break widely deployed public-key systems including RSA, Diffie-Hellman, and ECC. This has motivated extensive research on post-quantum cryptography (PQC) and quantum-based security mechanisms for future grid infrastructures. In this context, a Self-Defensive Post-Quantum Blockchain Architecture (SD-PQBA) has been proposed to protect SCADA systems against both classical cyberattacks and quantum-enabled cryptographic threats. This architecture integrates lattice-based and code-based cryptographic schemes with a novel Proof of Derived Authority (PoDA) consensus mechanism and employs a three-key (primary-private-public) cryptographic structure along with Quantum Key Distribution (QKD) to ensure data integrity and immutability. The proposed framework demonstrates resilience against false data injection, man-in-the-middle, denial-of-service, and malware attacks while maintaining low computational overhead suitable for real-time SCADA environments [36].

Lattice-based cryptography has emerged as a core building block for quantum-resistant smart grid security. A comprehensive survey of lattice-based security and authentication schemes highlights that cryptosystems based on hard lattice problems provide strong resistance against both classical and quantum attacks. The study further analyzes lattice-based protocols for key exchange, authentication, secure data aggregation, and privacy-preserving communication in IoT-enabled smart grid networks, showing that these approaches offer a favorable

balance between security strength and computational/communication cost compared to traditional public-key cryptography [37].

In addition to software-based cryptographic solutions, quantum cryptography offers unconditional security through the physical properties of quantum mechanics. A quantum-secure data transmission model combines Quantum Key Distribution (QKD) with classical One-Time Pad (OTP) encryption to protect smart meter data exchanged with utility providers. By utilizing Quantum Random Number Generators (QRNG), the model generates truly random encryption keys, eliminating the predictability of pseudo-random number generators and enabling the detection of eavesdroppers through the quantum no-cloning theorem. Experimental evaluations conducted on both classical simulators and real quantum hardware using the IBM Qiskit platform demonstrate that the proposed approach achieves lower computational cost than DES, AES, and RSA while providing stronger security guarantees. These results confirm the practical feasibility of deploying QKD- and QRNG-based secure communication channels in smart grids [38].

Beyond key generation and encryption, the reliable distribution of quantum resources across grid communication networks is also critical. An SDN-based entanglement routing framework supported by reinforcement learning has been proposed to enable distributed quantum sensing and entanglement-based key distribution in smart power grids. In this architecture, the SDN control plane maintains a global view of network conditions, including link noise levels and available qubit resources, and dynamically selects optimal entanglement distribution paths. Simulation results on an IEEE-14 bus power grid topology show that the reinforcement learning-based routing strategy achieves a 100% success rate for entanglement delivery under degraded link conditions, significantly outperforming traditional shortest-path routing algorithms [39]. This demonstrates that intelligent SDN-assisted control is essential for sustaining quantum-secure communications in realistic grid scenarios.

Despite these advances, challenges remain for the large-scale deployment of quantum-safe security in smart grids. The integration of QKD infrastructure and quantum servers into existing communication networks introduces cost, deployment, and interoperability constraints. Moreover, hybrid security architectures that combine PQC with QKD will be required to support heterogeneous grid devices with limited computational capabilities. Therefore, future research must focus on lightweight post-quantum protocols, SDN-assisted quantum resource management, and gradual migration strategies toward fully quantum-safe smart grid communication infrastructures.

3.7. Big Data Analytics

The modern smart grid is characterized by an explosion of data, from high-resolution sensor measurements to millions of smart meters logging usage data, to network devices recording traffic flows. If harnessed effectively, big data analytics can significantly improve situational awareness and threat detection in the grid. By aggregating and correlating data across the electrical, IT, and physical

domains, operators can identify anomalies or precursors to attacks that would be impossible to see in isolated data streams [40]. For example, a slight fluctuation pattern in voltage combined with unusual network traffic and some out-of-bounds control commands might together signal a coordinated cyber-physical attack.

Big data platforms can handle multi-source data streams in near real-time, applying ML or rule-based analytics to flag such complex events. In our multi-layer security model, a SIEM system enriched with big data capabilities can ingest logs and telemetry from all layers and produce a unified threat picture for analysts. However, realizing these benefits is challenging due to the classic “4 Vs” of big data (volume, velocity, variety, and veracity). The volume of data in a nationwide smart grid can be petabytes per day; storing and processing this cost-effectively requires scalable infrastructure and clever data reduction techniques. Velocity is also high – data streams need to be processed in seconds for effective intrusion detection, which calls for real-time stream processing engines rather than batch analysis. Variety is extreme: data formats range from time-series sensor data and IP network logs to unstructured data like maintenance reports or even social media. Ensuring data veracity (quality and trustworthiness) is non-trivial – sensors can be faulty or calibrated differently, and an attacker may try to feed false data to confound analytics. In short, big data analytics is a cornerstone for the future of grid security.

3.8. Enabling Technologies: Radio Frequency Fingerprinting

The nascent concept of radio frequency fingerprinting (RFF) for device identity has an important role to play in smart grid security. RFF is a signal intelligence method used to identify radio transmitting devices by extracting their unique characteristics. These unique features, or fingerprints, result from manufacturing imperfections in components like amplifiers, filters, and clock generators. These imperfections cause variations in signal characteristics such as phase offset, IQ imbalance, and clock skew. RFF enhances cybersecurity by providing a potential authentication technique for low-power, computation-constrained devices in next-generation networks, especially with the proliferation of IoT devices [41]. Unlike cryptographic methods with high computational overhead, RFF leverages a device's unique physical characteristics for lightweight authentication. While earlier RFF techniques relied on human-extracted features, the current trend is to employ AI, particularly DL, for feature extraction and classification [42]. From a cybersecurity perspective, RFF offers a robust layer of physical-layer security [43]. It can be used as an access control and anti-fraud measure, effectively identifying and preventing unauthorized devices from accessing network resources. This is particularly important for critical infrastructures like smart grids, where the cybersecurity of IoT devices is paramount [44, 45]. As a result, RFF represents forward-looking elements of grid security and adds an innovative layer of device integrity checking that complements digital authentication. By addressing both who can see data (privacy) and what a device physically is (fingerprinting), we cover dimensions often overlooked in traditional solutions,

moving closer to a comprehensive security and trust framework for future SDN-enabled smart grids.

Current literature heavily focuses on DL-based RFF methods, demonstrating relatively high performances, and seems to be the standard approach. However, the practical implementation of RFF may still face significant challenges. For example, the long-term reliability of RFF is questionable due to hardware aging. Degradation in functionalities of electronic components, for instance, crystal oscillators, leads to slowly varying features resulting in alterations of device fingerprints. Questions regarding classification accuracy and the sustainability of the RFF system have been raised. In particular, the long-term impact of aging is often ignored or not modelled in existing literature, which results in a critical gap in understanding the long-term viability of the RFF systems for sustainable IoT security. Another challenge could be feature drift, introducing a more complex conceptual ambiguity for RFF-authentication-based security. If device fingerprints alter and evolve due to aging and environmental interference, then long-term device discrimination may be inherently dynamic rather than static. These issues challenge widespread assumptions about permanent hardware identifiers. It also suggests that both security guarantees and privacy risks need to be considered in a time-varying context. Consequently, RFF should be analysed as both a static biometric identifier and a dynamic signal feature subject to physical evolution.

4. Discussion

The explanations in this study highlight that resilience in SDN-enabled smart grids cannot be achieved through isolated security mechanisms alone; instead, it depends on a coordinated defense-in-depth architecture spanning physical, cyber, and operational domains. By structuring protections across the Physical/Perception, Network/Communication, Control, and Application/Management layers, the proposed framework positions SDN's centralized programmability as a cohesive security orchestration mechanism rather than merely a network optimization tool. This layered integration enhances resistance to false data injection, man-in-the-middle attacks, denial-of-service disruptions, and malware propagation while preserving the strict latency requirements inherent in real-time SCADA operations.

At both the network and control layers, SDN introduces a structural shift from passive connectivity toward active, policy-driven enforcement. Programmable forwarding elements enable detection and mitigation functions to operate directly within the data plane, reducing response latency and supporting early containment of volumetric attacks through dynamic isolation and rerouting. Simultaneously, the integrity of the control layer—whose compromise could destabilize the entire system—must be continuously verified rather than implicitly trusted. Multi-factor authentication, cryptographic validation of control messages, runtime integrity attestation, and controller redundancy collectively reduce systemic vulnerability, while AI-assisted behavioural monitoring helps identify subtle misuse or insider threats. Although these safeguards introduce operational overhead, SDN's automation capabilities embed security enforcement within routine control workflows, preserving responsiveness.

Security at the physical edge further underscores the need for distributed verification. Deploying radio frequency fingerprinting at IoT gateways provides an additional identity assurance mechanism for resource-constrained devices, complementing traditional cryptographic approaches. However, hardware signatures evolve due to environmental variation and component aging, necessitating adaptive enrolment strategies and multi-factor validation—particularly in open-set environments where previously unseen devices must be assessed without prior reference.

At higher operational layers, visibility and governance must be balanced with privacy considerations. Role-based access control, tamper-evident logging, and explainable analytics strengthen accountability while enabling timely response within a zero-trust management paradigm. In parallel, blockchain technologies offer targeted value in scenarios where provenance and distributed trust are essential, such as verifying policy consistency across controllers or enabling secure information exchange in decentralized energy ecosystems. Their deployment in time-sensitive environments, however, must be carefully engineered through permissioned architectures and hybrid on-chain/off-chain designs to avoid compromising operational responsiveness. Privacy-preserving analytics and federated learning further ensure that enhanced situational awareness does not come at the cost of excessive data centralization.

The integration of advanced analytics introduces both opportunities and constraints. Generative AI, when bounded by explainability, uncertainty estimation, and human oversight, can synthesize heterogeneous operational data and support scenario-based training; yet uncontrolled deployment risks latency, opacity, or erroneous outputs. Similarly, quantum-resilient cryptographic approaches represent a gradual transition rather than an immediate replacement of existing mechanisms. Lattice-based post-quantum schemes provide near-term protection, while selective use of quantum key distribution may enhance confidentiality in critical channels. SDN's ability to orchestrate both classical and emerging quantum resources reinforces its role as a unifying coordination layer.

Big-data analytics extend cross-domain awareness by correlating electrical, cyber, and operational signals, transforming raw telemetry into actionable intelligence despite challenges related to scale, velocity, and reliability. Within this framework, advanced SIEM platforms evolve into genuine decision-support systems rather than mere alert aggregators.

Implementation must therefore proceed incrementally. Hybrid validation environments combining simulation, hardware-in-the-loop testing, and field pilots are essential to quantify resilience gains using measurable indicators such as recovery time, detection accuracy, and service continuity. Early deployment efforts should prioritize segmentation, gateway-level identity assurance, and lightweight auditing before progressing toward AI-assisted decision support or quantum-secure communication. Variations in technological maturity, legacy integration constraints, and workforce readiness remain practical limitations, while the long-term

stability of physical-layer identification methods and the operational feasibility of blockchain and quantum solutions warrant further empirical investigation.

Overall, these findings support a convergence-oriented security strategy in which SDN provides the structural foundation for coordinated enforcement, blockchain enhances integrity and traceability, advanced analytics improve interpretability, and emerging cryptographic approaches prepare infrastructures for future threat landscapes. The effectiveness of this approach lies not in any single technology but in its deliberate alignment under measurable performance and privacy constraints, enabling smart grids to strengthen resilience while maintaining the reliability and responsiveness essential to critical infrastructure.

5. Conclusion

The evolution of power grids into smart infrastructures requires equally smart and adaptive security strategies. In this paper, we presented a multi-layer security concept model for SDN-enabled smart grids that incorporates a spectrum of emerging technologies – from blockchain and XAI to quantum cryptography and device fingerprinting – each reinforcing different layers of defense. The central theme is defense-in-depth: a coordinated architecture of complementary measures to significantly strengthen grid security. At the network level, SDN provides agility and oversight for threat response, while at the data and control levels, AI-driven analytics and blockchain-enabled integrity create a trustworthy environment for decision-making. Physical layer and human factor security are strengthened through innovations like RFF and privacy-preserving data handling. We have also discussed open research challenges in integrating these technologies, such as scalability in blockchain, explainability in AI, quantum resistance, managing big data, and maintaining privacy.

To achieve effective integration, emerging technologies should not be seen in isolation but as parts of a cohesive model. This convergence of technologies, orchestrated in an SDN framework, offers a promising route to proactively defend against both current and future threats. The main challenges include technical maturity, interoperability, and the need for upskilling the workforce to manage these advanced tools. However, each challenge is an opportunity for innovation, from pilot deployments of XAI in grid operation centers to field tests of RF fingerprinting for grid IoT devices. We hope that this work contributes to the development of comprehensive security solutions for the grids of tomorrow.

Acknowledgements

This work has been supported by YÖK ADEP through the Gazi University Scientific Research Projects Coordination Unit under grant number FGA-2022-8043.

Author Contributions

S. Sağıroğlu: Supervision, project administration, conceptualization, methodology, validation.

M. Dener: Project administration, writing- review & editing.
A. Kara: Formal analysis, visualization, writing-review.
M. S. Demirci: Formal analysis, visualization, writing-review.
M. Demirci: Formal analysis, visualization, writing- review & editing, validation.
S. Yilmaz: Writing-original draft,
Y. Atay: Writing- review & editing.
S. Al: Writing-original draft.

Conflict of Interest

The authors declare no conflict of interest.

References

- [1] S. Demirci and S. Sağıroğlu, "Software-defined networking for improving security in smart grid systems," in *Proc. 2018 7th International Conference on Renewable Energy Research and Applications (ICRERA)*, Paris, France, 2018, pp. 1021–1026, doi: 10.1109/ICRERA.2018.8567005.
- [2] Y. Su, P. Jiang, H. Chen, and X. Deng, "A QoS-guaranteed and congestion-controlled SDN routing strategy for smart grid," *Applied Sciences*, vol. 12, no. 15, p. 7629, Aug. 2022, doi: 10.3390/app12157629.
- [3] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2637–2670, thirdquarter 2019, doi: 10.1109/COMST.2019.2908266.
- [4] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: a comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.
- [5] P. Ding, J. Li, L. Wang, M. Wen, and Y. Guan, "HYBRID-CNN: an efficient scheme for abnormal flow detection in the SDN-based smart grid," *Security and Communication Networks*, vol. 2020, p. 8850550, Aug. 2020, doi: 10.1155/2020/8850550.
- [6] S. Demirci, "QoS-Aware Routing Approaches in Software-Defined Smart Grids," in *Proc. 9th Int. Conf. Comput. Sci. Eng. (UBMK)*, 2024, pp. 982–987, doi: 10.1109/UBMK63289.2024.10773500.
- [7] F. Hauser, M. Häberle, M. Schmidt, and M. Menth, "A survey on data plane programming with P4: fundamentals, advances, and applied research," *Journal of Network and Computer Applications*, vol. 212, p. 103561, Mar. 2023, doi: 10.1016/j.jnca.2022.103561.
- [8] A. AlSabeH, J. Khoury, E. Kfoury, J. Crichigno, and E. Bou-Harb, "A survey on security applications of P4 programmable switches and a STRIDE-based vulnerability assessment," *Computer Networks*, vol. 207, p. 108800, Apr. 2022, doi: 10.1016/j.comnet.2022.108800.
- [9] M. E. Sahin and M. Demirci, "ConPoolUBF: connection pooling and updatable Bloom filter based SYN flood

- defense in programmable data planes," *Computer Networks*, vol. 231, p. 109802, Jul. 2023, doi: 10.1016/j.comnet.2023.109802.
- [10] P. Radoglou-Grammatikis, P. Sarigiannidis, T. Lagkas, and I. Moscholios, "SDN-based resilient smart grid: the SDN-microSENSE architecture," *Digital*, vol. 1, no. 4, pp. 173–187, Nov. 2021, doi: 10.3390/digital1040013.
- [11] Y. Y. Ghadi, T. Mazhar, T. Shahzad, M. A. Haq, and E. M. Tag-ELDin, "A hybrid AI-blockchain security framework for smart grids," *Scientific Reports*, vol. 15, no. 1, p. 20882, Feb. 2025, doi: 10.1038/s41598-025-05257-w.
- [12] R. Alsaigh, R. Mehmood, and I. Katib, "AI explainability and governance in smart energy systems: A review," *Frontiers in Energy Research*, vol. 11, p. 1071291, Feb. 2023, doi: 10.3389/fenrg.2023.1071291.
- [13] K. Singh and L. Sevukamoorthy, "Blockchain and AI-based threat detection for enhanced security in financial networks," in *Proc. IEEE TEMSCON-ASPAC*, Bengaluru, India, 2023, pp. 1–5, doi: 10.1109/TEMSCON-ASPAC59527.2023.10531316.
- [14] P. Kumar, R. Kumar, A. Aljuhani, D. Javeed, A. Jolfaei, and A. N. Islam, "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity," *Solar Energy*, vol. 263, p. 111921, Oct. 2023, doi: 10.1016/j.solener.2023.111921.
- [15] M. J. Islam, A. Rahman, S. Kabir, M. R. Karim, U. K. Acharjee, M. K. Nasir, and S. Wu, "Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3850–3864, Mar. 2022, doi: 10.1109/JIOT.2021.3107834.
- [16] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, and A. Mosavi, "Smartblock-sdn: An optimized blockchain-sdn framework for resource management in IoT," *IEEE Access*, vol. 9, pp. 28361–28376, Feb. 2021, doi: 10.1109/ACCESS.2021.3058225.
- [17] W. Li, Y. Wang, and J. Li, "A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems," *International Journal of Information Security*, vol. 22, no. 5, pp. 1219–1230, Oct. 2023, doi: 10.1007/s10207-023-00688-6.
- [18] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K. K. R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Computers & Security*, vol. 85, pp. 288–299, Aug. 2019, doi: 10.1016/j.cose.2019.05.006.
- [19] A. Jindal, G. S. Aujla, and N. Kumar, "SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," *Computer Networks*, vol. 153, pp. 36–48, Apr. 2019, doi: 10.1016/j.comnet.2019.02.012.
- [20] U. Ghosh, L. Njilla, S. Shetty, and C. A. Kamhoua, "A decentralized smart grid communication framework using SDN-enabled blockchain," in *Proc. 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2024, pp. 982–985, doi: 10.1109/CCNC57856.2024.10454790.
- [21] H. Xu, S. Wang, N. Li, K. Wang, Y. Zhao, K. Chen, and H. Wang, "Large language models for cyber security: A systematic literature review," *ACM Transactions on Software Engineering and Methodology*, vol. 33, no. 6, pp. 1–38, Jul. 2024, doi: 10.1145/3648438.
- [22] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4150, Jan. 2021, doi: 10.1002/ett.4150.
- [23] A. Adadi and M. Berrada, "Peeking inside the black-box: a survey on explainable artificial intelligence (XAI)," *IEEE Access*, vol. 6, pp. 52138–52160, Sep. 2018, doi: 10.1109/ACCESS.2018.2870052.
- [24] J. Gui, Z. Sun, Y. Wen, D. Tao, and J. Ye, "A review on generative adversarial networks: Algorithms, theory, and applications," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 4, pp. 3313–3332, Apr. 2023, doi: 10.1109/TKDE.2021.3130191.
- [25] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016, doi: 10.1109/TNNLS.2015.2474845.
- [26] R. Zhang, H. W. Li, X. Y. Qian, W. B. Jiang, and H. X. Chen, "On large language models safety, security, and privacy: A survey," *Journal of Electronic Science and Technology*, vol. 23, no. 1, p. 100301, Mar. 2025, doi: 10.1016/j.jnlest.2024.100301.
- [27] X. Yan and Y. Ding, "Are We There Yet? A Measurement Study of Efficiency for LLM Applications on Mobile Devices," in *Proc. 2nd International Workshop on Foundation Models for Cyber-Physical Systems & Internet of Things (FMCPS-IoT '25)*, May 2025, pp. 19–24, doi: 10.1145/3715015.3725062.
- [28] I. Naik, D. Naik, and N. Naik, "Threat Landscape of Adversarial Attacks on Generative AI and Large Language Models (LLMs): Exploring Different Types of Adversarial Attacks, Associated Risks, and Mitigation Strategies," *Authorea Preprints*, Jan. 2025, doi: 10.22541/au.173711927.42438865/v1.
- [29] K. Chahine, M. A. Sayed, A. Al-Ghadhban, and A. Al-Mogren, "Toward secure smart grid systems: risks, threats, challenges, and future directions," *Future Internet*, vol. 17, no. 7, p. 318, Jul. 2025, doi: 10.3390/fi17070318.
- [30] H. Sun, R. Q. Hu, and Y. Qian, "Towards enhancing security for upcoming 6G-ready smart grids: a

- hierarchical architecture," *Cybersecurity*, vol. 5, no. 1, p. 14, Dec. 2022, doi: 10.1186/s42400-022-00124-4.
- [31] N. Abdulla, S. Demirci, M. Demirci, and S. Özdemir, "Adaptive learning in IoT-based smart city applications," in *Principles and Applications of Adaptive Artificial Intelligence*, Hershey, PA, USA: IGI Global, 2024, pp. 73–101, doi: 10.4018/979-8-3693-1950-5.ch004.
- [32] A. Sarikaya, B. G. Kılıç, and M. Demirci, "RAIDS: robust autoencoder-based intrusion detection system model against adversarial attacks," *Computers & Security*, vol. 135, p. 103483, Dec. 2023, doi: 10.1016/j.cose.2023.103483.
- [33] M. K. Roshan and A. Zafar, "Boosting robustness of network intrusion detection systems: a novel two phase defense strategy against untargeted white-box optimization adversarial attack," *Expert Systems with Applications*, vol. 249, p. 123567, Sep. 2024, doi: 10.1016/j.eswa.2024.123567.
- [34] Y. Zhu, H. Wen, R. Zhao, Y. Jiang, Q. Liu, and P. Zhang, "Research on data poisoning attack against smart grid cyber-physical system based on edge computing," *Sensors*, vol. 23, no. 9, p. 4509, May 2023, doi: 10.3390/s23094509.
- [35] A. Alajaji, "FortiNIDS: Defending smart city IoT infrastructures against transferable adversarial poisoning in machine learning-based intrusion detection systems," *Sensors*, vol. 25, no. 19, p. 6056, Oct. 2025, doi: 10.3390/s25196056.
- [36] M. T. Naz, W. Elmedany, and M. Ali, "Securing scada systems in smart grids with iot integration: A self-defensive post-quantum blockchain architecture," *Internet of Things*, vol. 28, p. 101381, Dec. 2024, doi: 10.1016/j.iot.2024.101381.
- [37] H. Shekhawat and D. S. Gupta, "A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 14, p. e8080, Jun. 2024, doi: 10.1002/cpe.8080.
- [38] R. Rani, A. K. Singh, A. Parashar, and D. Saxena, "Quantum-Secure Data Transmission in Smart Grid," in *Proc. 2024 IEEE 17th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoc)*, Singapore, 2024, pp. 475–481, doi: 10.1109/MCSoc64094.2024.00078.
- [39] N. Skjellum, M. Shaban, and M. Ismail, "SDN-Based Entanglement Routing Strategy in Smart Power Grids Using Reinforcement Learning," in *Proc. 2025 IEEE International Conference on Quantum Computing and Engineering (QCE)*, Montreal, QC, Canada, 2025, vol. 2, pp. 133–138, doi: 10.1109/QCE61605.2025.10234.
- [40] Y. Maleh, Y. Qasmaoui, K. El Gholami, Y. Sadqi, and S. Mounir, "A comprehensive survey on SDN security: threats, mitigations, and future directions," *Journal of Reliable Intelligent Environments*, vol. 9, no. 2, pp. 201–239, Jun. 2023, doi: 10.1007/s40860-022-00171-8.
- [41] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges," *Computer Networks*, vol. 219, p. 109455, Dec. 2022, doi: 10.1016/j.comnet.2022.109455.
- [42] J. Zhang, G. Shen, W. Saad, and K. Chowdhury, "Radio frequency fingerprint identification for device authentication in the internet of things," *IEEE Communications Magazine*, vol. 61, no. 10, pp. 110–115, Oct. 2023, doi: 10.1109/MCOM.003.2200974.
- [43] M. A. Awan, Y. Dalveren, F. O. Catak, and A. Kara, "Deployment and implementation aspects of radio frequency fingerprinting in cybersecurity of smart grids," *Electronics*, vol. 12, no. 24, p. 4914, Dec. 2023, doi: 10.3390/electronics12244914.
- [44] M. Safi, S. Dadkhah, F. Shoeleh, H. Mahdikhani, H. Molyneaux, and A. A. Ghorbani, "A survey on IoT profiling, fingerprinting, and identification," *ACM Transactions on Internet of Things*, vol. 3, no. 4, pp. 1–39, Nov. 2022, doi: 10.1145/3539736.
- [45] A. Kara, "Practical implications of the use of radio frequency fingerprinting (RFF) in cybersecurity of smart grids," in *Proc. 4th IFSA Winter Conference on Automation, Robotics & Communications for Industry 4.0/5.0*, Innsbruck, Austria, Feb. 2024, pp. 112–116.