Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Review Article

Post-Quantum Secure Blockchain-Based Federated Learning Framework for Enhancing Smart Grid Security

Guma Ali [1,2,*], Kabiito Simon Peter[1], Maad M. Mijwil [3,4,5], Klodian Dhoska[6], Ioannis Adamopoulos [7,8]

[1] Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda
[2] Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India
[3] College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq
[4] Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq
[5] Faculty of Engineering, Canadian Institute of Technology, Albania
[6] Department of Mechanics, Polytechnic University of Tirana, Albania
[7] Department of Public Health Policy, Sector of Occupational & Environmental Health, School of Public Health, University of West Attica, 11521, Athens, Greece
[8] Hellenic Open University, School of Social Science, of MPH Postgraduate program of Public Health Policy, Patra, Greece

Corresponding author: a.guma@muni.ac.ug

ARTICLE INFO
Article History
Received: 15/08/2025
Accepted: 16/09/2025
Published: 30/09/2025

ABSTRACT
Emerging technologies have accelerated the digitalization of smart grids, improving demand-side management, sustainability, and operational efficiency. The attack surface is widened by this interconnection, though, leaving vital smart grid data and systems vulnerable to online attacks. Single points of failure, privacy violations, and a lack of robustness against sophisticated attacks persist in centralized data processing. Traditional cryptographic techniques are further threatened by the development of quantum computing, which raises significant security risks for smart grids. With a focus on post-quantum cryptography (PQC) resilience, this study examines 206 peer-reviewed research articles on blockchain-based federated learning (BFL) in smart grids that were published between January 2023 and July 2025. It assesses the advantages, limitations, and compromises of the current BFL models in this field. The paper suggests a unique post-quantum secure BFL (PQS-BFL) framework that integrates federated learning (FL), lightweight PQC protocols, and a scalable blockchain architecture to solve the vulnerabilities that have been uncovered. This design enables decentralized, private, and impenetrable cooperation among grid nodes. The results demonstrate that the system mitigates quantum-resilient attacks and inference threats while improving data integrity, key management, and secure model aggregation. A path for creating safe, scalable PQS-BFL solutions for upcoming smart energy systems is provided in the paper's conclusion, along with an overview of the main research issues. This study shows that using PQC, blockchain, and FL to secure next-generation smart grids is both feasible and important.

Keywords: *Smart grid, federated learning, blockchain, post-quantum cryptography, cybersecurity*

1. INTRODUCTION

The swift advancement in smart grids has transformed conventional power systems by integrating modern communication, sensing, and control technologies, enabling efficient, reliable, and sustainable energy management. Smart grids form interconnected electrical networks that use automation and modern technologies, such as sensors,

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

smart meters, cyber–physical systems, Internet of Things (IoT) devices, and control systems, interconnected through wired and wireless communication networks across three hierarchical layers: the home area network (HAN), neighborhood area network (NAN), and wide area network (WAN) [1-3] to ensure real-time monitoring and optimized energy distribution. These systems facilitate the integration of renewable energy sources, enhancing sustainability, availability, operability, reliability, and efficiency of power generation and distribution [4-8]. These systems facilitate the seamless integration of renewable energy sources and distributed energy resources (DERs), enhancing power availability, operational flexibility, and environmental sustainability [4-6]. The smart grid systems are supported by key technologies, including Advanced Metering Infrastructure (AMI), Distribution Automation (DA), Distributed Energy Resource Management Systems (DERMS), Energy Storage Systems (ESS), Electric Vehicles and Vehicle-to-Grid (V2G) systems, and Distribution Management Systems (DMS) [9-15]. By enabling bidirectional flows of electricity and data, smart grids modernize energy systems to support dynamic demand response, adaptive consumption, improved voltage regulation, and enhanced financial settlement mechanisms [6-8][16-19]. With global investment accelerating, valued at US$43.1 billion in 2021 and projected to reach US$103.4 billion by 2026 [20], smart grids represent a critical foundation for sustainable infrastructure development. While digitalization has brought unprecedented benefits to grid performance and management, the increased interconnectivity and real-time data exchange expose smart grids to a wide range of cybersecurity threats, including privacy violations, data breaches, reconnaissance and traffic analysis attacks, eavesdropping, insider threats, Man-in-the-Middle (MitM) attacks, spoofing, replay and password attacks, packet sniffing, side-channel and SQL injection attacks, False data injection and False command injection attacks, Aurora and Automatic Generation Control attacks, Time synchronization attacks, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, jamming, buffer overflow, teardrop, Smurf, and puppet attacks. Additional threats comprise masquerade attacks, advanced persistent threats, adversarial machine learning, grid balancing manipulation, protocol vulnerabilities, malware infections, session hijacking, supply chain compromises, physical intrusions, false pricing strategies, network flooding, social engineering, zero-day exploits, wormhole and covert attacks, load dropping, and smart meter tampering [6][8][21-23]. These threats can lead to severe consequences, including operational disruptions, theft of sensitive data, power outages, infrastructure damage, data breaches, and disruptions to critical services, ultimately threatening national security and public safety [6][8][23][24].

Several high-profile cyberattacks have exposed the vulnerabilities of smart grids and critical infrastructure worldwide. For example, in December 2020, attackers infiltrated thousands of networks through a malware-laced update from SolarWinds, a provider of network and device management software [25]. That same year, on October 12, hackers disrupted power in Mumbai, India, causing widespread outages and nearly paralyzing critical infrastructure. Between 2017 and 2018, Russian hackers launched a cyber espionage campaign targeting energy companies in the U.S. and Europe, utilizing spear-phishing and social engineering tactics to access sensitive industrial control data [25]. Finally, in 2015, the Black Energy virus struck Ukraine's power grid, causing outages in the Ivano-Frankivsk region and disrupting industrial production [26]. To prevent these attacks in smart grid systems, traditional centralized security models are ill-equipped to secure the decentralized, heterogeneous, and data-intensive nature of smart grids. In response, researchers have explored advanced techniques, including FL, blockchain, and PQC. FL enables edge devices to collaboratively train machine learning models without sharing raw data, preserving privacy while supporting real-time analytics. It is especially effective in latency-sensitive, bandwidth-constrained environments [27][28]. However, FL remains vulnerable to model poisoning, inference attacks, and manipulation of the aggregation process [29-32]. Blockchain integration enhances FL by offering decentralized trust, tamper-proof auditability, and verifiable updates. Through smart contracts and consensus mechanisms (e.g., Practical Byzantine Fault Tolerance, Proof of Stake), blockchain ensures secure coordination among grid participants [33]. However, traditional blockchain systems rely on cryptographic schemes like Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC), which quantum computers could potentially compromise using algorithms such as Shor's algorithm and Grover's algorithm. The emergence of quantum adversaries thus poses a threat to the foundational trust model of current blockchain architectures [34-37]. The emergence of quantum computing introduces risks to conventional cryptographic schemes, such as RSA and ECC [34][36]. To mitigate these, PQC techniques, including lattice-based, code-based, and hash-based algorithms, must be integrated into smart grid security architectures. Incorporating PQC into these systems can future-proof smart grid applications by securing model updates, enhancing edge device authentication, preserving long-term data privacy, enabling quantum-resilient secure aggregation, strengthening federated identity management, protecting communication channels, supporting blockchain-based auditing, improving key management, and ensuring regulatory compliance [5][38-42]. Integrating blockchain into FL for smart grids presents several limitations and trade-offs. These include challenges in maintaining data privacy, selecting suitable consensus protocols, and addressing vulnerabilities such as smart contract bugs, Sybil attacks, and 51% attacks. Additionally, integration can lead to computational inefficiencies and expose sensitive information, thereby posing a risk to confidentiality. To address these gaps, this study proposes a PQS-BFL framework for enhancing the security of smart grids. This framework

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

combines decentralized learning, quantum-resistant security, and immutable auditability to protect sensitive energy data and enable resilient, real-time decision-making. The proposed framework strengthens smart grid security by enabling secure decentralized learning, applying PQC safeguards, managing trust and participant authentication, preserving data privacy, and implementing effective incentive and reward mechanisms. It ensures tamper-resistant auditability and logging, enhances resilience to model poisoning and Byzantine attacks, and supports scalable and interoperable operations across grid entities. By integrating these capabilities, PQS-BFL delivers quantum-resistant security, decentralized trust, privacy-preserving model aggregation, robust protection against adversarial threats, transparent auditing, efficient key management, enhanced data integrity, improved scalability, and adherence to regulatory standards.

Although researchers have individually explored FL, blockchain, and PQC within the context of smart grids, few studies unify these components into a single, cohesive, and secure framework. This review addresses that gap by proposing a PQS-BFL architecture designed explicitly for next-generation smart grid security. The paper presents a comprehensive framework that integrates FL, blockchain, and PQC mechanisms to secure smart grid applications. It investigates key security and privacy challenges within smart grids, reviews current approaches to integrating FL and blockchain, and examines their vulnerabilities in the face of quantum threats. The review also explores emerging PQC solutions relevant to BFL, identifies open research challenges, and outlines potential future directions. There are a few related research papers that emphasize the urgent need to integrate quantum-resistant security into FL systems for smart grids. For instance, Ahmad et al. [43] conducted a thorough survey on smart microgrid security using blockchain-enabled FL with quantum-safe techniques. Similarly, Ren et al. [44] introduced a novel quantum-secured distributed intelligent system for smart cyber-physical dynamic security assessment (DSA), which combines FL and quantum key distribution, referred to as quantum-secured federated DSA (QFDSA). Despite these advancements, most existing studies fall short of delivering a fully integrated security architecture that simultaneously incorporates (i) FL, (ii) PQC, and (iii) blockchain-based verification and consensus. Furthermore, few frameworks are tailored explicitly to the unique infrastructure and threat models of smart grids. This research bridges that gap by presenting a unified, PQS-BFL framework designed to meet the evolving security demands of smart grid systems.

This study provides a holistic review with the following contributions:

- To assess the evolving cybersecurity threats in smart grids.
- To analyze FL's role in enhancing privacy and explore its inherent limitations in security and trust assurance.
- To explore blockchain's integration with FL, including how distributed ledger technologies enhance trust, traceability, and resilience in collaborative learning.
- To critically evaluate the vulnerabilities of current blockchain and FL frameworks to quantum computing threats and justify the need for PQC enhancements.
- To design a PQS-BFL framework for enhancing smart grid security and identifying their roles and benefits in smart grid security.
- To identify technical challenges, trade-offs, and open research problems, offering recommendations for future research directions in secure, scalable, and quantum-resilient smart grid ecosystems.

The remainder of this paper is structured as follows. Section 2 details the materials and methods employed in the study. Section 3 reviews the current state-of-the-art in smart grids, while Section 4 explores cybersecurity considerations within smart grid systems. Section 5 discusses the application of FL in smart grids, and Section 6 analyzes how blockchain supports secure and transparent FL. Section 7 addresses quantum threats and introduces PQC primitives relevant to smart grid security. Section 8 proposes a taxonomy for a PQS-BFL framework tailored to smart grids. Section 9 presents real-world implementations and case studies of such frameworks, while Section 10 outlines the key challenges and unresolved issues associated with their deployment. Section 11 recommends future research directions, and Section 12 concludes the study.

2. MATERIALS AND METHODS

This study systematically investigates PQS-BFL frameworks within the context of smart grid security. Recognizing the multidisciplinary nature of the topic, the methodology integrates a comprehensive literature review, bibliometric analysis, and thematic synthesis to ensure thorough coverage, objectivity, and conceptual clarity. The review focuses on the convergence of PQC, blockchain technology, and FL as applied to smart grid environments. Given that quantum computing poses serious threats to conventional cryptographic schemes and smart grids increasingly rely on distributed learning systems, the study critically examines cutting-edge frameworks that integrate these three technologies. It identifies current trends and architectural designs that support secure and privacy-preserving FL, evaluates blockchain's role in enabling decentralized coordination, and explores how PQC can mitigate emerging quantum

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

threats. To conduct the review, the researchers performed an extensive search across major scientific databases and digital libraries, including PLoS ONE, Frontiers, SAGE, Wiley, Nature, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, and Google Scholar. The search was limited to peer-reviewed journal articles and conference papers published between January 2023 and July 2025. Energy systems, cybersecurity, electrical engineering, and computer science were among the pertinent fields. The researchers customized keyword strings and Boolean combinations for each database to optimize the search process and increase the likelihood of a successful search. They used queries like "federated learning" or "collaborative learning" AND ("blockchain" or "distributed ledger") AND ("post-quantum cryptography," "quantum-resistant," "lattice-based cryptography," "code-based cryptography," or "hash-based signatures") AND ("smart grid," "intelligent energy systems," or "cyber-physical systems") AND ("privacy," "security," "robustness," or "trust management" AND". Only the most pertinent research was included once these queries had been revised to match each platform's indexing syntax. The researchers used stringent inclusion and exclusion criteria to ensure the quality and applicability of the chosen literature. They included only publications that addressed blockchain-enabled FL frameworks; applications of PQC schemes in FL or blockchain systems; or cybersecurity challenges and solutions in smart grid environments involving AI, FL, or distributed ledger technologies. Peer-reviewed journal articles and credible conference papers from accredited institutions that displayed methodological rigor and technical innovation were considered. Only publications in English, with full-text access available through institutional subscriptions or open-access platforms, were considered. The review focused on literature published between January 2023 and July 2025 to capture recent advances. The selected studies had to explicitly or implicitly apply to smart grid systems, such as smart meters, DERs, demand response, or grid-edge intelligence, and prioritize security aspects, particularly those related to post-quantum resilience and privacy-preserving distributed learning. Preference was given to research presenting conceptual models, prototypes, algorithms, or real-world implementations that contribute significant theoretical or empirical insights into smart grid security. The researchers excluded studies that lacked relevance, technical rigor, or up-to-date insights. Specifically, they removed research focused solely on blockchain or FL without precise application to smart grid security or PQC contexts, as well as studies on PQC with no practical integration into distributed learning or blockchain systems. They also excluded research studies with superficial content, such as high-level overviews, marketing whitepapers, or works lacking cryptographic proofs, system architecture diagrams, or performance evaluations. Outdated surveys, redundant publications with minimal content variation, and studies published before January 2023 that failed to reflect recent advancements were also omitted. Non-English sources, inaccessible publications without institutional or open access, and non-peer-reviewed grey literature, such as blogs, opinion pieces, and informal reports, were excluded.

The researchers employed a multi-phase process comprising identification, initial screening, eligibility assessment, and final inclusion, ensuring transparency, consistency, and reproducibility throughout the review. Three independent reviewers conducted the search, extracted relevant metadata, and analyzed the technical content of each study. The data extraction focused on publication details, FL models, blockchain consensus mechanisms, PQC primitives, smart grid applications (e.g., load forecasting, intrusion detection), and security/privacy guarantees. To organize their findings, the researchers categorized the literature into five thematic dimensions: (1) cryptographic foundations, (2) FL models, (3) blockchain integration, (4) smart grid applications, and (5) security, privacy, and fairness guarantees. They also implemented test-retest validation by re-evaluating a subset of studies to minimize bias and enhance reliability. The initial search yielded over 4,798 publications. After removing duplication and abstract screening, the pool narrowed to 2,964 studies. From these, 938 studies passed the eligibility assessment, and 206 publications met the final inclusion criteria. These works were thematically categorized and analyzed for their relevance to the core focus of PQS-BFL in smart grid systems. The selected studies included 2 from PLoS ONE, 3 from Frontiers, 1 from SAGE, 10 from Wiley, 4 from Nature, 6 from Springer, 29 from ScienceDirect, 39 from MDPI, 81 from IEEE Xplore Digital Library, and 31 from Google Scholar. Fig. 1 presents a summary of their categorization and relevance to the research focus.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

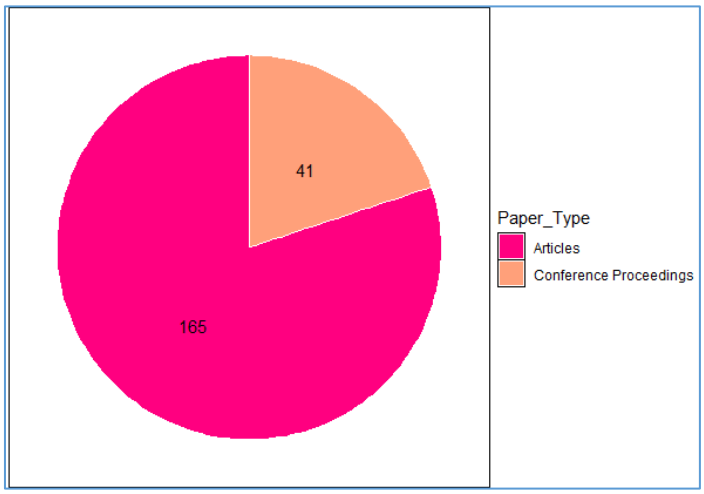

Fig. 1. Categorizes the research papers selected for the study.

Fig. 2 presents the digital databases used to retrieve the research papers included in this review.

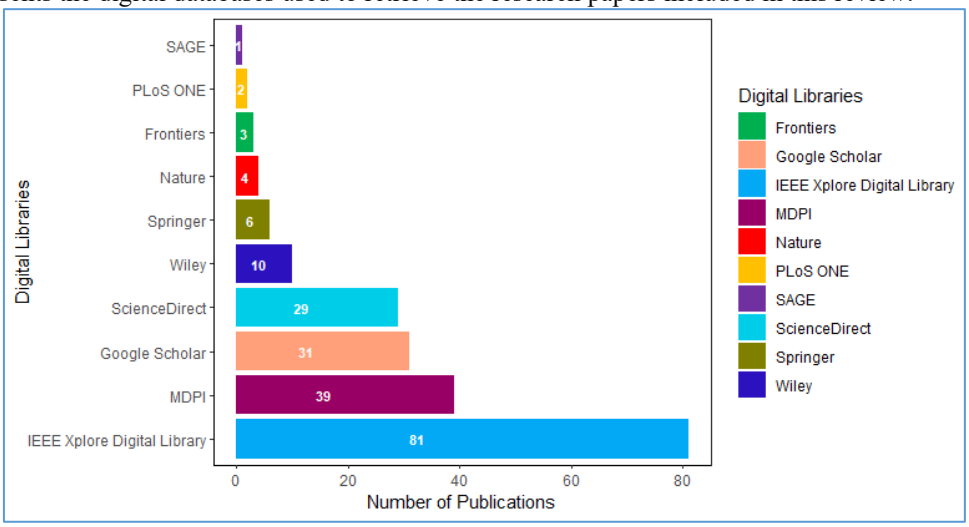

Fig. 2. Illustrates the digital databases from which the selected research papers were retrieved.

Fig. 3 illustrates the distribution of research papers across various digital libraries.

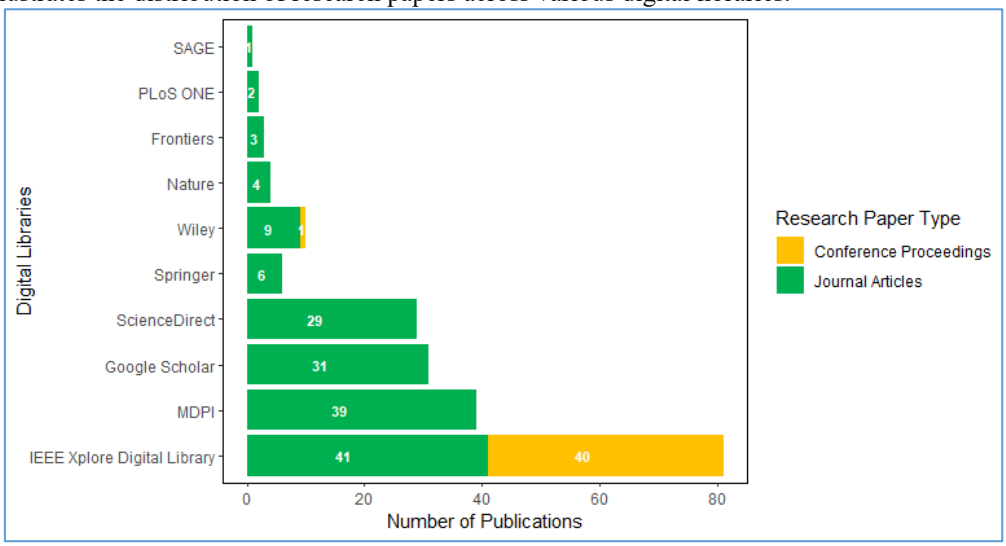

Fig. 3. Illustrates the distribution of research papers across various digital libraries.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Fig. 4 illustrates the distribution of the selected papers across publication years, based on data collected from various digital libraries.

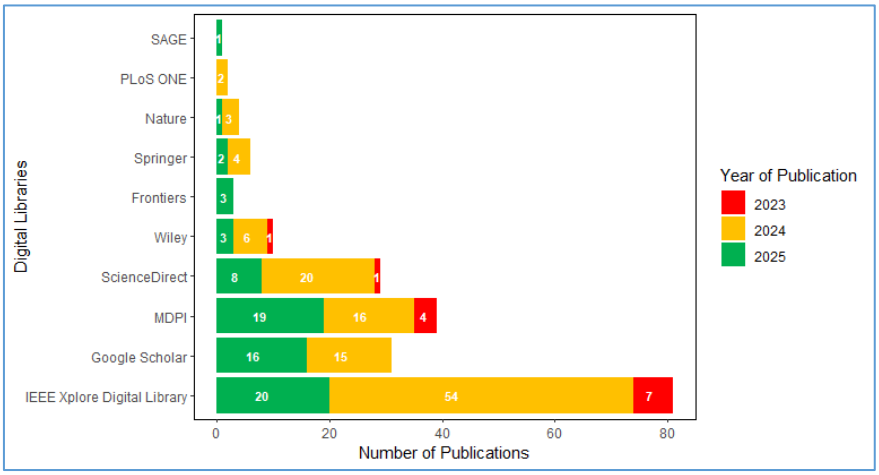

Fig. 4. Illustrates the distribution of selected papers from various digital libraries across publication years.

Given the interdisciplinary nature of the topic, the researchers employed a narrative synthesis approach, guided by a thematic coding framework, to extract qualitative insights. They began with thematically clustering studies based on the primary integration level of BFL components. Examples included the application of PQC-enhanced blockchains in FL training and the use of FL in blockchain-supported intrusion detection systems within smart grids. Through cross-study comparisons, the researchers identified architectural patterns, cryptographic strategies, and performance trade-offs, which allowed them to map trends and highlight divergences across the reviewed literature. To evaluate each study, the team considered technology readiness levels, practical applicability in real-world smart grid environments, and associated deployment challenges. They also assessed methodological rigor using a grading system that prioritized research quality, relevance to PQS-BFL frameworks, and the reliability of reported findings. This evaluation highlighted key gaps, including the lack of robust PQC integration, insufficient energy efficiency benchmarking, and persistent scalability limitations. Drawing on these insights, the researchers synthesized recurring future research directions into actionable recommendations, emphasizing the need for standardization, interoperability, and the development of quantum-resistant cryptographic primitives.

In addition to the thematic analysis, the researchers validated their conclusions through expert consultation and comparison with prior studies. By analyzing the consistency and robustness of the examined data, they critically evaluated the quality of their conclusions. They made sure that all sources were properly cited and only included peer-reviewed research that was published between January 1, 2023, and July 31, 2025, to preserve quality and relevance. Because the study only used previously published research, ethical approval was not necessary. Notwithstanding its methodological merits, this review contains a number of shortcomings that compromise the thoroughness and relevance of its conclusions. First, the review might not include the most recent developments or new issues because PQC, blockchain, and cybersecurity technologies are evolving so quickly. The incorporation of varied international perspectives is limited by the sole concentration on English-language periodicals. It's possible that the dependence on major academic databases left out pertinent research from specialized or niche sources. The evaluation also ignores insights from industry reports, white papers, and preprints, which frequently offer important practical knowledge, by limiting the analysis to peer-reviewed literature. By leaving out foundational studies published before 2023, which could provide important historical context, the selected era further reduces the scope. The study's conclusions are less statistically sound because it mostly used qualitative evaluations and did not use empirical or quantitative data. Furthermore, the research prioritized theoretical suggestions over practical implementation concerns, including user acceptability, scalability, deployment cost, and energy usage. Lastly, synthesis was hampered by the variation in study quality, which resulted from variations in technique, research design, and reporting standards. Future cybersecurity risks that are outside the purview of this assessment may surface as a result of the continuous developments in artificial intelligence (AI) and quantum computing.

3. STATE-OF-THE-ART

3.1. Introduction to Smart Grid

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

The transformation of conventional electric power systems into intelligent, dynamic, and decentralized energy networks is exemplified by the smart grid. It improves the long-term sustainability, dependability, and efficiency of power generation, distribution, and consumption by utilizing automation and digital communication technology [4][5][7]. The smart grid, a next-generation system designed for resilience and adaptation, guarantees real-time distribution depending on demand by coordinating energy flow from several decentralized sources. A network of intelligent sensors at the center of this system coordinates energy output from dispersed generating facilities and precisely controls the distribution of electricity. By continuously monitoring production and consumption throughout the grid, these sensors make energy metering possible. The smart grid includes "prosumers"—entities that both create and use electricity—in addition to conventional producers and consumers. Prosumers can feed surplus energy back into the grid or draw from it when their demand exceeds local production [20][45-47].

The grid integrates DERs, such as solar and wind power, and manages them using smart meters, IoT devices, and sensors. These components collect time-series data on power flow, voltage levels, and consumption patterns. The central control system then analyzes this data in real time to detect anomalies, power fluctuations, or cybersecurity threats, ensuring the grid remains secure and stable [48]. A defining feature of the smart grid is its bidirectional flow of both electricity and information. This capability enables automated energy delivery, enhances demand-side management, and supports self-healing mechanisms for grid protection. Smart devices, including sensors, actuators, and meters, work in unison to monitor, balance, and control energy flow, making user and supplier behavior more transparent and manageable [14][49]. The smart grid's power flow framework consists of three main stages. First, during generation, energy is produced either centrally or locally, such as through residential solar panels. Real-time information and communication technologies (ICT) regulate production and enable feedback to the grid. Second, in the transmission and distribution stage, electricity flows through transformers, transmission lines, substations, and digital fault relays. ICT tools remotely manage these components to ensure safe and efficient delivery of services to end users. Finally, in the consumption stage, individuals, industries, and public institutions utilize electricity [50]. Some devices, such as electric vehicles, can return excess power to the grid through vehicle-to-grid communication, contributing to a more flexible and balanced energy system. Fig. 5 shows the conceptual illustration of the smart grid.

Fig. 5. Shows the conceptual illustration of the smart grid.

Smart grids represent a transformative evolution of traditional power systems. By integrating advanced digital communications, real-time data exchange, and automation technologies, they significantly enhance the efficiency, reliability, and sustainability of electricity generation, distribution, and consumption [1][14][19][25][51-53]. Unlike conventional unidirectional grids, smart grids enable two-way flows of both electricity and information. This capability allows for real-time monitoring, dynamic load balancing, demand-response strategies, and decentralized energy

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

generation [54-56]. These advanced systems utilize intelligent devices, such as sensors, smart meters, and automated switches, to optimize energy usage, minimize transmission losses, and facilitate predictive maintenance and fault detection [57-59]. Smart grids give utility companies and consumers more precise control over energy supplies by implementing technologies like AI, big data analytics, cloud computing, and the IoT [22][60–62]. This integration increases the adoption of electric vehicles, lowers greenhouse gas emissions, and encourages energy conservation [63]. Smart grids incorporate DERs, such as renewable energy sources, and employ ubiquitous control systems to optimize grid operations dynamically, in addition to technical developments. They use sensitive sensors, automated controls, and real-time data to improve system efficiency and dependability. Demand-side response initiatives, smart appliance integration, and cutting-edge energy storage technologies like plug-in electric and hybrid cars are all supported by these networks. Traditional electromechanical grids, which rely on centralized generation and limited control capabilities, are fundamentally different from smart grids. Because of their self-monitoring, self-healing, and bidirectional communication features, they can quickly adjust to errors or disruptions. To enhance demand-side management, consumers gain from comprehensive energy usage data, cost transparency, and incentives that promote changing consumption patterns. Additionally, the smooth integration of various and sporadic energy sources is made possible by technologies like energy storage devices, micro-generation systems, and smart meters. This plug-and-play feature encourages technological diversity and creativity. Power rerouting, autonomous operation when required, and energy asset management based on real-time system requirements are all capabilities of smart grids. These characteristics improve operational effectiveness and resistance to physical attacks, natural disasters, and cyber threats. Finally, with enhanced transmission capacity, integrated demand response, and a wider choice of energy services, smart grids improve market participation and guarantee power quality appropriate for contemporary digital technology [14][61]. They are the foundation of safe, robust, and sustainable energy infrastructure because of their intelligence, scalability, and adaptability [64][65].

3.2. Smart Grid Technologies

A variety of cutting-edge technologies that improve the effectiveness, dependability, and flexibility of power systems are necessary for efficient control and automation in smart grids. Real-time monitoring, intelligent control, and predictive maintenance are made possible by these technologies, which range from AMI and DA to complex software platforms like DMS and Energy Management Systems (EMS). They offer demand-side management and dynamic pricing, automate problem detection and service restoration, and enable two-way communication between utilities and customers. [9][14][19][64]. Situational awareness and operational coordination are further improved through integration with systems like Geographic Information Systems (GIS), Outage Management Systems (OMS), and Supervisory Control and Data Acquisition (SCADA). When combined, these solutions enhance customer interaction and service dependability, update grid operations, and simplify asset management [56][66][67]. The integration of DERs, electric vehicles (EVs), and energy storage devices is key to the development of the smart grid. Real-time grid balancing, bidirectional energy flow, and the smooth coordination of dispersed assets are made possible by technologies like Automatic Generation Control (AGC), V2G systems, and DERMS [10][11][68-70]. With the help of synchronized monitoring and high-resolution data from Phasor Measurement Units (PMUs) and Wide Area Management Systems (WAMS), utilities are able to control grid stability and react quickly to disruptions. Demand-side technology, on the other hand, such as time-of-use pricing, smart meters, and Home Energy Management Systems (HEMS), enables customers to take part in energy management, lowering peak demand and increasing grid flexibility. Together, these systems optimize energy distribution, encourage better energy consumption, and increase resilience to the growing integration of renewable energy sources [13][14][56]. In addition to developing digital technologies like the IoT, edge computing, big data analytics, AI, and blockchain, this ecosystem is supported by fundamental enablers, including communication infrastructure, cybersecurity technologies, standards, and protocols. In addition to facilitating autonomous control, decentralized energy trading, anomaly detection, and predictive decision-making, these components guarantee safe, scalable, and real-time data interchange [19][71–76]. Together, these technologies drive the evolution of smart grids into intelligent, adaptive, and sustainable energy systems.

3.3. Smart Grid Architecture

Smart grid architecture integrates traditional electrical power systems with advanced digital communication, control, and automation technologies within a multi-layered framework that enables bidirectional energy and data flows. This architecture enhances reliability, efficiency, and the integration of DERs, EVs, and demand-side management. It operates on core principles such as interoperability, scalability, reliability, resilience, security, privacy, and decentralization, ensuring seamless interaction among diverse systems and stakeholders, by supporting functional and capacity growth, maintaining stability under varying conditions, defending against cyber threats, and enabling distributed generation, storage, and control. Each layer of the architecture performs distinct but interrelated functions that collectively advance the smart grid's performance. Below are brief descriptions of these layers.

3.3.1.Physical layer

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

The physical layer underpins smart grid architecture by integrating hardware, infrastructure, and transmission media to enable real-time sensing, measurement, control, and communication of electrical and data signals. Serving as the interface between the physical environment and the grid's digital systems, it facilitates data acquisition, command execution, signal transmission, and power delivery. Smart meters, sensors, actuators, PMUs, remote terminal units (RTUs), intelligent electronic devices (IEDs), energy storage systems, and electric vehicle supply equipment (EVSE) are some of the devices that fall under this layer. To ensure dependable connectivity across a range of grid configurations, these components interact via conventional media, such as fiber optics, power line communication, and Ethernet, as well as wireless technologies, such as Wi-Fi, ZigBee, 5G, LoRaWAN, and satellite communication. To improve data collection and facilitate intelligent monitoring and control throughout the smart grid, it also integrates IoT-based sensing technologies, such as RFID tags, wireless sensor networks, cameras, global positioning systems (GPS), and machine-to-machine (M2M) systems [21].

3.3.2.Sensing and measurement layer

The crucial connection between the digital intelligence that drives contemporary smart grid operations and the actual grid infrastructure is made by the sensing and measurement layer. To improve visibility, facilitate quick defect detection, and aid in effective decision-making, it records real-time data on power flow, system status, environmental factors, and energy consumption. Monitoring electrical parameters (voltage, current, frequency, and power factor), identifying and localizing issues, gathering data for advanced analytics, and enabling automated control actions like load shedding and voltage regulation are just a few of the important tasks carried out by this layer. The core components, including smart meters, PMUs, IEDs, RTUs, and a range of sensors, collaborate to deliver granular monitoring and control across the grid. These devices incorporate various communication technologies, including Ethernet, Wi-Fi, LTE, Zigbee, and LoRaWAN, and comply with industry protocols such as IEC 61850 and DNP3 to ensure interoperability and reliable data exchange. By providing accurate, timely insights into grid conditions, equipment health, and consumption patterns, the sensing and measurement layer underpins automation, reliability, and energy efficiency in smart grid systems [77][78].

3.3.3.Communication layer

The communication layer serves as the smart grid's nervous system, enabling secure, reliable, and real-time data exchange across all components and layers. It links generation units, substations, control centers, DERs, EVs, smart meters, and consumer devices to ensure seamless coordination and interoperability. As smart grids become more complex and decentralized, this layer plays a vital role in supporting functions such as monitoring, control, automation, demand-side management, real-time pricing, outage detection, and predictive maintenance. It transmits data between physical devices, such as sensors and actuators, and processing systems, coordinates activities across grid segments—generation, transmission, distribution, and consumption—and bridges diverse platforms and protocols. Smart grids utilize both wired technologies, including fiber optics for high-speed backbone communication, Programmable Logic Controller (PLC) for cost-effective transmission over power lines, and Ethernet in substations, as well as wireless technologies such as ZigBee, Wi-Fi, 4G/5G/LTE, LoRaWAN, and NB-IoT for applications ranging from HAN to WAN. Telecommunication infrastructure enhances this layer's reliability, facilitates analog-to-digital conversion, and supports rapid, intelligent responses. Additionally, the network layer forwards data from the perception layer to the application layer, utilizing short-range technologies such as Bluetooth and ZigBee, as well as long-range options like Wi-Fi, 5G, and PLC, to ensure efficient data transport under various constraints [21][58].

3.3.4.Data management layer

The data management layer is crucial to smart grid architecture, enabling efficient acquisition, preprocessing, storage, analysis, and dissemination of vast, heterogeneous data streams across the energy ecosystem. It collects and aggregates data from DERs, smart meters, sensors, EVs, and substations, and filters, cleans, normalizes, and synchronizes this information before storing it using scalable solutions such as cloud, edge, or hybrid systems. Leveraging advanced analytics and modeling, it facilitates load forecasting, fault detection, demand response, and energy flow optimization. The layer distributes processed data to higher-level applications and control systems, supporting visualization, alerts, and automated decision-making. By managing diverse data types, including operational, consumer, market, environmental, and cybersecurity data, and integrating big data technologies, utilities can predict system behavior, enhance grid performance, and drive data-informed operational strategies [58][61].

3.3.5.Control layer

The control layer serves as the operational core of the smart grid, managing, optimizing, and coordinating the real-time behavior of diverse grid components. It connects the physical infrastructure, such as power generation units, substations, distribution networks, and end-user devices, with the digital intelligence layer, which includes AI, analytics, and decision support systems. Leveraging real-time data and hierarchical control strategies enables dynamic, adaptive, and automated grid operations. Key functions include supervisory control and data acquisition, real-time

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

voltage and frequency regulation, load forecasting, demand-side management, grid balancing, ancillary services, and fault detection, isolation, and restoration. Organized into three hierarchical levels—primary (local device or substation control), secondary (regional coordination and stability), and tertiary (system-wide optimization and strategic planning)—the control layer plays a critical role in maintaining grid reliability. As smart grids become increasingly decentralized and complex, utilities rely on this layer, enhanced by edge computing and AI-driven automation, to monitor performance, resolve faults, optimize energy distribution, and maintain a real-time balance between supply and demand [58].

3.3.6.Application layer

The application layer, the topmost tier of smart grid architecture, interfaces directly with end-users, such as consumers, utilities, and operators, connecting them to the underlying data, communication, and control systems. It integrates operational technology (such as grid control and energy management systems) with information technology (including analytics platforms and user portals) to deliver real-time services that enhance grid management, improve energy efficiency, facilitate user interaction, and support informed decision-making. This layer transforms inputs from lower levels into actionable services that enable automation, visualization, and customer engagement. By leveraging advanced digital technologies, such as AI and machine learning for predictive maintenance and optimization, big data analytics to handle vast datasets, and web or mobile platforms for real-time control and monitoring, it ensures seamless interoperability across diverse systems through APIs and middleware. The application layer also enables real-time monitoring, active demand management, outage response, and asset optimization by working with components such as software-defined networking (SDN) controllers and dashboards that visualize network performance and alert operators to critical events. Additionally, it employs IoT technologies to monitor and troubleshoot smart grid devices, defining sensor data acquisition through its application infrastructure and service-linked servers. As smart grids evolve toward decentralized, data-driven models, this layer plays a critical role in delivering secure, interoperable, and AI-enabled functionality essential for building a resilient and sustainable energy system [21][61].

3.3.7.Security and privacy layer

The security and privacy layer safeguards the smart grid by ensuring the integrity, confidentiality, and availability of its data and systems. As smart grids incorporate advanced ICT infrastructure, cloud services, IoT devices, and DERs, they face increasing risks of cyberattacks, data breaches, and privacy violations. This layer uses PQC solutions like CRYSTALS-Kyber and CRYSTALS-Dilithium, strong security frameworks, and encryption protocols like Advanced Encryption Standard (AES), RSA, and ECC to lessen these threats. Additionally, it makes use of real-time intrusion detection systems and secure communication standards as IEC 62351, Transport Layer Security (TLS), and Internet Protocol Security (IPsec). It enforces strict authentication, authorization, auditability, and accountability while leveraging blockchain technology for decentralized security. Privacy-preserving techniques, such as data aggregation, anonymization, FL, and user-centric access controls, protect personal information without hindering analytics. The layer ensures compliance with standards such as NISTIR 7628, IEC 62443, ISO/IEC 27001, and privacy regulations, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), thereby strengthening governance and regulatory compliance. By adopting a security-by-design approach, automating incident response, and continuously monitoring threats, it maintains resilient and trustworthy smart grid operations. Supported by identity management, firewalls, and network monitoring, these cybersecurity measures fortify the grid against digital threats and enhance public confidence in smart grid technologies [58][61].

3.3.8.Regulatory and policy layer (Overarching)

The regulatory and policy layer, also referred to as the overarching layer in smart grid architecture, shapes the planning, operation, and development of smart grids by establishing the legal, institutional, market, and policy frameworks that align the grid with societal, economic, and environmental objectives. This strategic governance tier directs and constrains the physical infrastructure, communication systems, and operational controls, ensuring compliance with national and regional laws while protecting consumer rights and data privacy. It promotes fair market competition and transparency through regulatory oversight, policy development, market and tariff design, stakeholder coordination, and enforcement of standards and interoperability. By setting clear rules for innovation, renewable integration, and grid modernization, this layer drives sustainable energy transitions, enhances system reliability and security, and fosters collaboration among utilities, regulators, technology providers, and consumers. It also addresses critical challenges such as data privacy, cybersecurity, and the integration of distributed energy resources, supporting a resilient and future-ready energy ecosystem [79][80]. Fig. 6 illustrates the key layers that make up the smart grid architecture, highlighting how each layer contributes to the grid's overall functionality.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

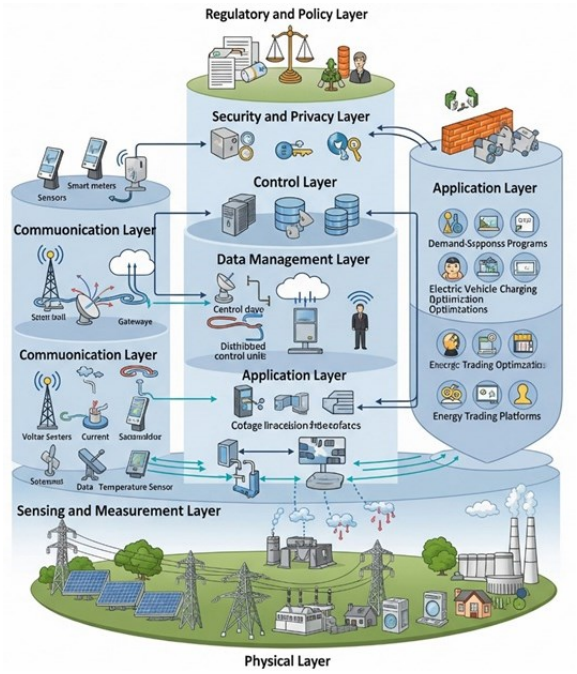

Fig. 6. Illustrates the primary layers of the smart grid architecture.

3.4. Communication Technologies in Smart Grids

The traditional electricity grid transmits electricity from power plants to substations via high-voltage transmission lines and delivers it to residential, commercial, and industrial consumers through low-voltage distribution networks. However, these conventional grids typically lack communication capabilities at the distribution level and consumer premises. On the other hand, smart grids use cutting-edge communication technologies that allow houses, smart meters, appliances, and grid stations to share data in both directions. By easing the integration of renewable energy sources and improving overall stability and resilience, this communication infrastructure helps the grid to better manage, control, and monitor its components. Three tiers make up the hierarchical structure of smart grid communication: HAN, NAN, and WAN. Each tier is intended to satisfy particular needs and applications.

3.4.1. Home Area Network

By facilitating real-time, two-way communication between smart meters, home appliances, energy management systems, and utility providers in residential settings, a HAN is an essential component of the smart grid communication infrastructure. Demand response, dynamic pricing, and the integration of dispersed energy resources, such as battery storage and rooftop solar panels, are all supported. HANs enable comprehensive energy monitoring, appliance automation, and load management based on user preferences or utility signals by connecting smart devices via a central gateway, usually the smart meter. Using short-range communication technologies like Zigbee, Wi-Fi, and Bluetooth, these networks typically span regions of less than 200 square meters and operate at low data speeds (10–100 kbps). HANs allow utilities to do remote diagnostics, firmware updates, and secure data transmission while empowering consumers to effectively manage energy consumption through in-home displays and smart applications. HANs, the innermost layer of the smart grid architecture, work in tandem with NANs and WANs to create a complete ecosystem that improves energy efficiency, grid resilience, and real-time grid interaction. [1][2][45][81][82].

3.4.2. Neighbour Area Network

By acting as an intermediary layer connecting several HANs to the utility's WAN, a NAN is essential to smart grid connectivity. For real-time monitoring, control, and management, it collects data from sensors, smart meters, and DERs and sends it to utility control centers. Depending on capacity, latency, and deployment needs, NANs use a mix of wired and wireless technologies, including radio frequency mesh, Wi-Fi, Zigbee, 5G, or fiber optics, to span limited areas of less than 10 km. NANs enable utilities to control devices such as load switches and streetlights remotely, support demand response signals, and facilitate event reporting for outages or tampering incidents. Designed as mesh, hierarchical, or hybrid networks, they offer scalability and low latency, supporting thousands of nodes. Smart meters function as both data sources and network nodes, forwarding data to concentrators, which then send it to the meter data management system. By bridging communication between end-user devices and core utility systems, NANs form the distribution layer of the smart grid and ensure its reliable operation [1][2][45] [82-84].

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

3.4.3. Wide Area Network

The WAN serves as the core tier of the smart grid communication architecture, acting as the backbone that connects widely dispersed nodes, such as substations, control centers, data concentrators, power plants, and distributed energy resources, across large geographic areas. It delivers high-capacity, long-range, and low-latency communication essential for real-time grid monitoring, control, and automation. WANs support mission-critical operations, including SCADA functions, fault detection, state estimation, and wide-area protection, while also facilitating demand response and the integration of renewable energy sources. To meet these demanding needs, WANs employ a combination of advanced wired and wireless technologies to ensure reliability, scalability, security, and interoperability. By linking NANs, HANs, and core utility systems, WANs enable the seamless exchange of large volumes of operational and metering data, making them indispensable to maintaining the stability, efficiency, and intelligence of modern power grids [1-3][64][82][85]. Communication technologies generally fall into two categories: wired and wireless.

3.4.4. Wired technologies

Wired communication technologies are essential to smart grid systems, providing reliable, high-bandwidth, and interference-resistant connections that are crucial for demanding environments such as substations, control centers, and distribution automation systems. Optical Fiber Communication enables high-speed, low-latency data transmission over long distances with electromagnetic immunity, making it indispensable for mission-critical applications despite high costs and installation complexity [86][87]. PLC leverages existing power lines to transmit data cost-effectively, supporting smart metering and automation while facing challenges such as noise and interference, which hybrid solutions help mitigate [88]. Digital Subscriber Line (DSL) utilizes existing copper telephone lines to provide scalable, affordable connectivity for smart meters and control centers. However, its performance declines over distance, and it is more vulnerable to interference compared to fiber [89][90]. Ethernet (IEEE 802.3) provides robust, scalable, and high-speed networking, widely used in substations and control systems, and is enhanced by protocols such as IEC 61850 and Time-Sensitive Networking, enabling reliable, time-critical communication [91]. Serial communication standards RS-232 and RS-485 continue to provide a simple, durable, and cost-effective means of data exchange for field-level devices and legacy systems, with RS-485 being favored for its noise resilience and multi-drop capability [92][93]. Lastly, coaxial cables, although legacy technology, remain valuable in specific smart grid applications, such as AMI and video surveillance, especially where existing infrastructure can be reused, offering moderate bandwidth and strong electromagnetic shielding despite limitations in scalability and signal attenuation. Together, these wired technologies strike a balance between performance, cost, and deployment considerations to support the evolving communication needs of smart grids.

3.4.5. Wireless technologies

Wireless technologies are crucial for smart grid communication, enabling reliable, scalable, and flexible data exchange among grid components without the need for extensive physical infrastructure. Utilities deploy these technologies across various smart grid layers—HAN, NAN, and WAN—to support critical applications such as demand response, outage management, AMI, and real-time monitoring and control. Wi-Fi (IEEE 802.11) offers high data rates and ease of deployment for short-range, non-critical tasks, but it faces challenges related to interference, range, and power consumption [87]. Zigbee (IEEE 802.15.4) excels in low-power, low-data-rate applications within HANs, offering mesh networking, strong security, and long battery life, although it struggles with interference and limited throughput [64][87]. Wireless Mesh Networks (WMNs) enhance coverage and resilience through decentralized, self-healing, multi-hop communication, making them ideal for AMI and distribution automation despite bandwidth and energy constraints [89]. Cellular networks (3G, 4G, 5G) provide wide-area coverage, high throughput, and mobility support, which benefits real-time grid protection and DER integration; however, they also entail subscription costs and cybersecurity concerns [64][87]. Narrowband IoT (NB-IoT) offers energy-efficient, interference-resistant connectivity for massive low-throughput devices, supporting mission-critical smart grid functions with extended battery life. However, its low data rates limit the application of time-sensitive controls [94]. Satellite communication ensures reliable, global coverage for remote areas, integrating with terrestrial networks to enhance resilience and disaster response, while facing latency and cost challenges that newer low-earth orbit constellations aim to overcome [71][95]. WiMAX (IEEE 802.16) offers high-speed, long-range connectivity suitable for wide-area smart grid applications but contends with spectrum licensing and competition from LTE/5G [64]. Bluetooth Low Energy (BLE) supports low-power, short-range communication for residential HANs and IoT devices, with expanding mesh capabilities despite limited range and susceptibility to interference [64][96]. WLAN (Wi-Fi-based) networks facilitate high-speed, short-range communication within HAN and field area network (FAN), evolving to overcome earlier limitations through innovations like mesh topologies and power-saving protocols [64]. Z-Wave offers a low-power, sub-GHz mesh protocol designed for home automation and energy management, minimizing interference while being limited in bandwidth and range [64]. 6LoWPAN enables IPv6-based communication over low-power IEEE 802.15.4 networks,

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

supporting scalable, IP-compatible smart grid deployments while facing bandwidth and security challenges [64]. LoRa and LoRaWAN provide low-power, long-range LPWAN connectivity with scalable and secure architectures, making them ideal for rural smart grid sensing and control applications. However, their limited throughput and latency make them unsuitable for real-time applications [64]. SigFox offers ultra-narrowband, low-data-rate communication with wide coverage and minimal infrastructure, successfully connecting millions of IoT devices for smart metering and environmental monitoring [64]. Neul exploits TV white space spectrum to provide low-power, long-range connectivity with superior signal penetration, presenting a promising, though still developing, LPWAN alternative for smart grid applications. Together, these wireless technologies form a diverse ecosystem that utilities tailor to meet the varying requirements of coverage, power consumption, data rate, latency, security, and deployment cost across smart grid environments [64].

3.5. Cyber Threat Landscape in Smart Grids

The digital transformation of traditional power systems into smart grids has brought about greater efficiency, automation, and data-driven decision-making; however, it has also significantly increased their vulnerability to cyber threats. Below are the detailed descriptions of the key cyber threats in smart grids:

3.5.1. Privacy attack

Smart grids improve the efficiency, reliability, and sustainability of electricity distribution, but they also expose systems to serious cybersecurity threats, most notably privacy attacks. Adversaries target the detailed, real-time energy usage data collected by smart meters, sensors, and communication networks to infer sensitive personal information such as household occupancy, daily routines, appliance usage, and socioeconomic status. Non-intrusive load monitoring (NILM), which leverages models like temporal convolutional networks, enables attackers to deduce appliance-level activities and user habits without physical intrusion. Additional threats, including traffic analysis, data mining, insider misuse, data interception, and unauthorized profiling, further compromise data confidentiality and undermine consumer trust. The practicality of these attacks is illustrated by real-world events like the DEF CON smart meter hacking and the 2012 German research. Legal ramifications and a reduction in public confidence in smart grid technology are just a few of their effects, which also include hazards to personal safety and discriminatory actions by employers or insurance [25][97].

3.5.2. Data breach

Because they allow unauthorized access to sensitive data, including operational details, energy usage trends, and personal information, data breaches pose a serious threat to smart grid systems. To get access to these networks, attackers frequently take advantage of insider threats, weak communication protocols, and system flaws. Smart grids are more vulnerable due to their large attack surface, integration of legacy systems, and intricate networks of networked devices like sensors and smart meters. Once entered, attackers can compromise data confidentiality, integrity, and availability, change meter readings, limit communications, or interfere with services. Weak authentication, insecure APIs, and inadequate encryption have made it possible for data exfiltration and operational disruptions, as evidenced by real-world events such as the 2016 German utility breach, the 2019 UK smart meter data leak, and the 2015 Ukrainian power grid attack. These hacks result in financial losses, operational instability, privacy violations, and a drop in customer confidence in smart grid technologies [98].

3.5.3. Reconnaissance attacks

The cybersecurity of smart grids is seriously threatened by reconnaissance attacks, which start the cyberattack lifecycle. Without creating any immediate disruption, attackers gather vital information about the target system's devices, communication protocols, architecture, and security measures during this phase, either actively or passively. By identifying network topologies, counting IP addresses and open ports, identifying device types and firmware versions, analyzing encryption techniques and communication protocols, and assessing security configurations like firewall rules and access controls, they seek to map the digital environment. Passive reconnaissance utilizes non-intrusive methods, including traffic sniffing and metadata analysis, to monitor communication patterns. In contrast, active reconnaissance employs direct probing techniques, such as port scanning, vulnerability scanning, and ping sweeps, using tools like Nmap and Nessus. In smart grids, attackers might scan substations for unauthenticated Modbus services, intercept unencrypted smart meter traffic to extract usage patterns or cryptographic keys, or analyze SCADA-RTU communications to infer control logic for future spoofing attacks. Malicious insiders may leverage internal access to expose firewall settings or access credentials. Although reconnaissance does not inflict direct damage, it lays the groundwork for targeted and disruptive attacks, such as DoS, MitM, and false data injection (FDI). Because of their high level of connection, dependence on legacy equipment, and insufficient separation of information technology (IT) and operational technology (OT) systems, smart grids are particularly susceptible to this crucial early stage of cyber-attack. [99]

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

3.5.4. Traffic analysis attack

A traffic analysis attack is a passive cyber threat in which adversaries monitor network traffic to gather intelligence without modifying the data, thereby compromising confidentiality and integrity. Attackers can deduce sensitive operational information, including occupancy patterns, appliance usage, energy load fluctuations, and production schedules, by looking at communication frequency, packet sizes, transmission timing, routing paths, and device interaction patterns. For example, an attacker can determine when residences are empty or when particular appliances are in use by monitoring smart meter traffic, which allows for targeted phishing efforts or physical incursions. Attackers can discover substation control cycles and emergency response protocols in SCADA systems by examining the timings and packet sizes of encrypted control signals. In the same way, keeping an eye on communications between distribution management systems and solar inverters can reveal DER scheduling and grid-balancing involvement, opening the door to potential market manipulation or operational disruption. These attacks compromise customer information, expose utility tactics, allow for targeted cyber intrusions, and run the danger of breaking regulations like the GDPR and the Critical Infrastructure Protection (NERC CIP) program of the North American Electric Reliability Corporation. Traffic analysis attacks can provide vital information, including node identities, IP addresses, physical locations, and communication roles, despite their passive nature and apparent lack of operational impact. This is particularly true in wireless sensor networks where key nodes are exposed by predictable routing paths [21][22].

3.5.5. Eavesdropping attack

Unauthorized parties secretly listening in on device-to-device conversations without changing the data being sent is known as eavesdropping. There is a serious risk to security and privacy in smart grids, which depend on two-way digital communication for effective energy management and distribution. Attackers exploit weak encryption, intercept wireless transmissions between smart meters and utilities, compromise routers or gateways, or tap into substation links to gather sensitive information. Such surveillance can expose household energy usage patterns, enable targeted attacks, such as MitM or replay attacks, support industrial espionage, and pave the way for active system manipulation. Real-world incidents have exposed vulnerabilities in smart meters that utilize unencrypted protocols, such as Zigbee, and in SCADA systems that rely on outdated standards, including Modbus and DNP3. Eavesdroppers can also analyze network traffic to infer grid topology and operational details, or to manipulate energy theft detection systems. Although it involves no direct interference, eavesdropping severely undermines confidentiality, integrity, and system accountability [21-23][55][100].

3.5.6. Insider threats

Insider threats present a significant and multifaceted risk to smart grids, stemming from individuals within the organization, such as employees, contractors, vendors, or partners, who possess legitimate system access but may misuse it either maliciously or through negligence. These threats include malicious insiders driven by financial motives or revenge, negligent users who disregard cybersecurity best practices, and compromised individuals whose credentials have been hijacked by external attackers. Smart grids are particularly vulnerable due to their integration of IT and OT, dependence on interconnected third-party vendors, high-privilege access granted to operators and engineers, and the critical need for uninterrupted real-time operations. Real-world incidents highlight the profound impact of insider threats. For example, ex-employees have retained system access after termination, credential sharing has opened the door to phishing attacks, third-party contractors have introduced malware, and administrators have unintentionally installed Trojan-infected software. These actions have disrupted operations, exposed sensitive data, harmed reputations, and caused significant financial losses [101].

3.5.7. Man-in-the-Middle attack

A MitM attacker infiltrates communication between smart grid entities, such as smart meters, control centers, and distributed energy resources, by secretly intercepting, modifying, or injecting data without the knowledge of the parties involved. By exploiting vulnerabilities such as weak authentication, unencrypted protocols, or insecure wireless links, the attacker eavesdrops on sensitive information, alters consumption data or control commands, replays captured messages, and impersonates legitimate devices using techniques like IP or ARP spoofing. This attack compromises the confidentiality, integrity, and availability of the smart grid, leading to fraudulent billing, disrupted grid operations, exposed consumption patterns, and eroded trust in the system. To execute a MitM attack, the adversary first gains network access and reroutes traffic to intercept bidirectional data flows, often targeting critical components like SCADA systems, RTUs, or PMUs. These attacks degrade system performance, conceal faults, and pave the way for further cyber threats [21-23][49][55][88][102][103].

3.5.8. Spoofing attack

Spoofing attacks pose a significant threat to smart grids, allowing attackers to impersonate legitimate devices or users by using falsified data, identities, or communication sources. These attacks target the critical communication networks linking smart meters, sensors, control centers, and DERs. By injecting counterfeit messages or commands, attackers

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

disrupt grid operations, manipulate control functions, steal sensitive data, and gain unauthorized access. The most common spoofing techniques include IP spoofing, GPS spoofing (which compromises timing synchronization in devices such as PMUs), data spoofing, and command spoofing. These methods enable the injection of false data, grid instability, financial losses, and privacy violations. For instance, GPS spoofing can desynchronize measurements, causing protective relay failures, while falsified meter readings can facilitate billing fraud [21][22][88].

3.5.9. Replay attack

An attacker launches a replay attack by intercepting and recording valid communications between smart grid devices, then retransmitting these messages later to trick the system into accepting them as new, legitimate commands. By exploiting the absence of proper authentication or timestamping, the attacker manipulates control signals, sensor data, or billing information, thereby disrupting operations through incorrect load management, false energy consumption reports, or misleading grid status updates. These attacks specifically target critical components such as smart meters, IEDs, and PLCs, granting unauthorized access, enabling data manipulation, and even causing physical damage to the grid. Because the replayed messages appear legitimate and comply with normal communication protocols, traditional detection methods often fail to recognize these threats, allowing attackers to inflict financial losses, operational instability, and data integrity breaches without requiring detailed knowledge of the system [21-23][49][77][102-104].

3.5.10. Packet sniffing

Attackers pose a serious threat to smart grids by intercepting and monitoring data packets traveling through the network—a practice known as packet sniffing, network sniffing, or packet capturing. Exploiting vulnerabilities such as ARP spoofing or MitM attacks, they actively or passively capture packets to extract sensitive information like real-time energy consumption, control commands, authentication credentials, and network configurations. This unauthorized access compromises user privacy, enables the injection of false data to disrupt grid operations, facilitates credential theft for unauthorized system access, and can lead to DoS attacks. Real-world incidents reveal how attackers have used wireless sniffers to collect unencrypted meter data for privacy invasion, manipulated control commands through ARP spoofing to trigger outages, and exploited weakly encrypted SCADA communications to breach control systems. Because smart grid communications often lack robust encryption, attackers frequently target devices such as PMUs and smart meters to intercept critical data unlawfully, thereby setting the stage for more severe threats, including FDI attacks [21][22].

3.5.11. Password attacks

Password attacks pose a significant threat to smart grids by exploiting weak or stolen authentication credentials to gain unauthorized access to critical systems and networks. Attackers employ techniques such as brute-force attacks, dictionary attacks, credential stuffing, phishing, social engineering, and password spraying to compromise user accounts. Social engineering stands out by manipulating human interaction to trick authorized users into revealing passwords, complementing technical methods like password guessing and sniffing. After obtaining valid credentials—often through theft—attackers manipulate grid operations, steal sensitive data, and move laterally within networks to escalate privileges or deploy malware. High-profile incidents, including the Ukraine power grid attacks and breaches caused by default passwords on smart meters, demonstrate how these tactics enable attackers to disrupt operations and undermine infrastructure security [21][22][49].

3.5.12. Side-channel attack

Attackers exploit unintended physical emissions, such as power consumption, electromagnetic radiation, timing variations, and acoustic signals—from smart grid devices like smart meters, sensors, and controllers to extract sensitive information. By analyzing these physical characteristics during cryptographic operations, they recover secret keys, authentication tokens, or operational data, allowing them to steal customer privacy information, manipulate data, impersonate devices, or disrupt grid stability. The most common attack methods include power analysis, electromagnetic analysis, and timing attacks that specifically target embedded cryptographic modules in smart meters and household appliances. Researchers have shown that monitoring power usage or capturing electromagnetic emissions can reveal encryption keys, while timing variations in communication protocols leak partial secrets. These vulnerabilities enable adversaries to bypass security controls, compromise administrative access, and undermine the reliable operation of smart grids [21][49].

3.5.13. False data injection attack

FDI attacks pose a stealthy and highly sophisticated cyber threat to smart grid systems by manipulating or fabricating measurement data from sensors, meters, or communication networks, thereby misleading the state estimation process, which is crucial for grid monitoring, control, and decision-making. To evade conventional bad data detection methods, attackers create fake data that is consistent with the grid's mathematical model. This deceives operators into making poor choices, such as wrong load balancing, unnecessary generation, or false alarms. These adversaries, who frequently

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

have only a limited understanding of the grid topology, target components such as buses, generators, transformers, and smart meters. By doing so, they can cause overload conditions or skew load distribution, which can result in equipment failures, blackouts, cascading outages, financial losses, and a decline in confidence in smart grid technologies. Through academic experiments, IEEE test systems, and actual events like the Ukraine power grid attack, researchers have illustrated a variety of FDI attack scenarios; sophisticated variations like zero-dynamic and load redistribution attacks highlight their growing complexity and peril [21–23].

3.5.14. False command injection attack

Attackers can implant illegal or misleading commands into communication channels that link control centers with devices like smart meters, sensors, and actuators, thanks to false command injection attacks (FCIAs), which are a serious cyber threat to smart grid control systems. To secretly alter grid operations, attackers take advantage of software flaws, mimic control signals, or intercept and alter valid directives. They can cause outages, harm equipment, interfere with power distribution, and destabilize frequency and voltage levels by imitating legitimate instructions. FCIAs directly interfere with command execution, unlike FDIAs that target sensor data, which makes detection more challenging and may have a more severe effect. Real-world incidents, including the 2015 Ukraine power grid attack, the Maroochy water system breach, the Aurora experiment, and the Stuxnet worm, highlight the devastating consequences of FCIAs on critical infrastructure. Furthermore, research simulations have demonstrated how attackers exploit compromised communication protocols, such as DNP3 and IEC 61850, to inject false commands, resulting in load imbalances and device failures [105].

3.5.15. Aurora attacks

Aurora attacks represent a cyber-physical threat that targets the OT of electric power grids, particularly within smart grid infrastructures. By manipulating control commands to critical components such as circuit breakers, transformers, and generators, attackers can cause physical damage and trigger widespread blackouts. First demonstrated in the 2007 “Aurora Vulnerability” test by Idaho National Laboratory, these attacks exploit vulnerabilities in communication protocols and control systems to send malicious commands—often overriding protective relays and forcing breakers to open or close out of sync with the grid. This deliberate desynchronization induces electrical faults, overheating, and severe mechanical stress on equipment, potentially leading to catastrophic failures. Unlike conventional IT attacks, which focus on data breaches, Aurora attacks directly damage physical infrastructure, blurring the boundary between the cyber and physical domains. The real-time, bidirectional communication in smart grids further expands the attack surface, especially when security measures are inadequate. While the 2015 Ukraine power grid attack was not a pure Aurora incident, it highlighted similar vulnerabilities. In a typical attack scenario, an adversary infiltrates a utility’s SCADA system, turns off the synchronism-check relay, and rapidly opens and closes a breaker while the generator remains out of phase. Attackers exploit this window to incorrectly resynchronize the generator, exposing it to damaging mechanical stress, because safety relays usually postpone tripping by roughly 15 cycles to prevent false positives [24][104].

3.5.16. Automatic generation control attacks

By regulating the output of several generators, Automatic Generation Control (AGC) is essential to preserving the real-time balance between the supply and demand for power. To maintain grid dependability, it controls tie-line power flows across interconnected control areas and stabilizes system frequency. AGC systems are becoming more and more vulnerable to cyberattacks as smart grids become more digitalized and linked via communication networks. Attackers can take advantage of these flaws to interfere with AGC operations by sending out illegal commands, replaying signals, jamming communications, or injecting fake data. Such behaviors may cause frequency instability, generation imbalances, equipment overloads, cascading failures, or widespread blackouts by misleading controllers into making the wrong changes. Frequency collapse can result from FDI, as shown by simulated scenarios and documented events like the 2015 Ukraine grid attack. Additionally, adversaries have attacked DNP3 and IEC 60870-5-104, two communication protocols. The lack of robust verification and detection techniques leaves AGC systems especially vulnerable. An attacker masquerading as a generator, for instance, may input persistently erroneous power flow data over several cycles or surpass its allotted timetable, disrupting the system without setting off warnings [24].

3.5.17. SQL injection attack

A common and dangerous cyberattack known as SQL injection (SQLi) inserts malicious SQL code into input fields or API requests to target database-driven systems. Because smart grids rely on interconnected components like smart meters, sensors, control centers, and databases that handle sensitive data like operational commands and customer information, this threat is especially serious. Attackers exploit poor input validation in login forms, data entry fields, and APIs to manipulate backend queries, enabling them to access, modify, or delete data, bypass authentication, and execute administrative commands that can disrupt grid operations. Smart grids remain highly vulnerable because they often integrate legacy systems with insecure code, operate across distributed architectures with multiple access points,

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

and follow inconsistent security standards across utilities. For example, the 2019 breach of a European utility's customer portal, along with research that demonstrated the alteration of smart meter readings or grid component shutdowns via SQLi, highlights the seriousness of the threat. These attacks compromise data integrity and system functionality, allowing adversaries to simulate normal operations while triggering outages or manipulating billing, undermining the reliability of the smart grid [21][49].

3.5.18. Time synchronization attack

A time synchronization attack (TSA) poses a significant cyber threat to smart grids by manipulating or spoofing critical timing signals from sources such as the GPS and the Network Time Protocol (NTP). Since smart grids rely on precise timing for coordinated operations, accurate monitoring, and effective fault detection, TSAs undermine these functions by deceiving PMUs, IEDs, RTUs, and other timing-dependent components into accepting false timestamps. Attackers achieve this by spoofing GPS signals or altering NTP packets, which causes devices to report inaccurate data, misalign measurements, and disrupt control commands, leading to distorted synchrophasor data, misinformed grid operators, obscured fault sequences, false alarms, and improper relay actions, ultimately jeopardizing grid stability and protection. Experiments in the real world have demonstrated that GPS spoofing on PMUs can mimic blackout circumstances by introducing phase angle issues and causing cascading failures from timing errors. Voltage instability, false fault isolation, diminished situational awareness, and significant financial losses can all be caused by TSAs. By targeting PMUs and wide-area measurement systems (WAMSs), these attacks also compromise location data, communication integrity, and voltage stability control, posing a significant threat to the integrity, availability, and reliability of smart grid operations [21][22][49][106].

3.5.19. Denial-of-Service and Distributed Denial-of-Service attacks

By flooding vital components with unauthorized traffic, DoS and DDoS attacks seriously compromise the availability and dependability of smart grid infrastructures by preventing legitimate users from accessing them. DoS attacks impair critical functions, including real-time monitoring, status estimation, and control by flooding control centers, data aggregators, or gateways with excessive requests or malicious packets from a single source. By focusing on communication levels like AMI, SCADA, and wide area monitoring systems, DDoS attacks, which are initiated by several hacked devices (botnets), increase their impact and make identification and mitigation more difficult. Inaccurate state predictions, missing or delayed control commands, cascading failures, and even widespread blackouts are frequently the results of these attacks. Attackers exploit vulnerabilities in protocols such as IEC 61850, IEEE C37.118, and DNP3, as well as in devices like PMUs, IEDs, and smart meters. They employ techniques such as TCP SYN flooding, buffer overflows, signal jamming, and MAC-layer spoofing to compromise both the physical and cyber layers of the grid, resulting in financial losses, performance degradation, and reputational harm [21-23][107].

3.5.20. Jamming attack

Jamming attacks target the wireless communication channels essential to smart grid operations by emitting high-power interference signals that disrupt or block legitimate transmissions. Exploiting the shared nature of wireless media, such as ZigBee, Wi-Fi, RF communication, and cellular networks, these attacks prevent smart meters, sensors, and control systems from exchanging critical data. By overwhelming the signal-to-noise ratio, attackers hinder the transmission of control commands and monitoring information, which degrades grid performance, delays fault detection, and can even trigger blackouts. Techniques include constant noise transmission, deceptive signal injection, intermittent jamming to evade detection, and reactive jamming triggered by legitimate activity. Real-world cases highlight these vulnerabilities: jamming ZigBee networks disrupts AMI, sensor network attacks blind control centers, and interference with 4G/5G impedes substation communication. Advanced methods, such as the Maximum Attacking Strategy using Spoofing and Jamming (MAS-SJ), corrupt time-synchronized PMU data in cognitive radio networks, while patterned jamming manipulates power pricing and undermines utility reliability. Because attackers only need access to the communication channel—not the network itself—jamming poses a high-severity threat despite its moderate likelihood. These attacks not only compromise service availability but also force devices to increase transmission power, driving up energy consumption. Strengthening smart grid resilience against such threats remains critical for preserving operational integrity and reliability [21][22].

3.5.21. Buffer overflow attacks

Buffer overflow attacks pose a significant cybersecurity threat to digital infrastructures such as smart grids by exploiting programming flaws that allow excess data to overwrite adjacent memory. This manipulation can alter program behavior, corrupt data, or enable the execution of malicious code. Smart grids remain especially vulnerable due to their complexity and exposure. Attackers often exploit these systems through remote code execution in SCADA components, manipulation of IEDs, or targeting AMI. Researchers have demonstrated that attackers can exploit flaws in communication protocols and firmware, or use malformed packets, to crash devices, gain unauthorized access, or manipulate billing information. These intrusions can destabilize the grid, corrupt critical data, cause device failures,

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

introduce persistent malware, and degrade network-layer communication. Furthermore, buffer overflow attacks can bypass passive intrusion detection systems and facilitate DoS attacks, compromising the availability, integrity, and confidentiality of smart grid operations [21][22].

3.5.22. Teardrop attack

A Teardrop attack is a DoS technique that exploits how specific operating systems reassemble fragmented IP packets. Instead of sending properly sequenced fragments, attackers craft malformed packets with overlapping or incorrect offset values, which older or unpatched systems often cannot process correctly, causing the targeted system to crash, freeze, or reboot unexpectedly. In smart grid environments—where real-time IP-based communication underpins devices such as smart meters, SCADA systems, IEDs, and AMI, such attacks pose a significant risk. Simulated attacks and research demonstrate that malformed packets can disrupt substation functions, turn off AMI communication hubs, and repeatedly crash legacy IEDs. These vulnerabilities persist due to outdated firmware, heterogeneous device configurations, broad attack surfaces, and constrained processing resources that limit effective threat detection and mitigation. By manipulating packet header lengths and fragmentation offsets, attackers can exploit these systemic weaknesses to destabilize grid operations [21].

3.5.23. Smurf attack

A Smurf attack is a type of DDoS attack that exploits the Internet Control Message Protocol (ICMP) and IP broadcast addressing to overwhelm a target system with traffic, rendering it unresponsive. The attacker spoofs the victim's IP address and sends ICMP Echo Request packets to the network's broadcast address, prompting all connected devices to respond simultaneously to the spoofed IP address. This amplification floods the victim's network with traffic. In smart grids, where real-time communication among smart meters, sensors, and control systems depends on IP networks, Smurf attacks exploit vulnerabilities such as legacy broadcast-capable devices, weak network segmentation, and spoofable protocols like ICMP. Attackers can hijack IoT devices to flood DMS, target gateways to disrupt smart meter networks, or overload SCADA servers in renewable energy systems. These attacks disrupt communication, delay fault detection and response, and increase the risk of power outages, operational blind spots, and grid instability [21].

3.5.24. Puppet attack

A puppet attack occurs when an adversary covertly exploits a legitimate or compromised device within a smart grid network to execute malicious actions without detection. By taking control of trusted nodes, such as smart meters, sensors, or relay devices, attackers manipulate commands, falsify data, or launch additional attacks while avoiding direct interaction with the control center. These compromised devices, often equipped with valid credentials and persistent malware, relay commands indirectly to obscure the origin of the attack. Adversaries target vulnerabilities in components such as AMI, SCADA systems, and DERs by injecting malware, exploiting firmware flaws, or leveraging insider threats. For instance, hijacked smart meters can send false consumption data or engage in DoS attacks; compromised DER inverters can destabilize the grid or propagate malware; and substation relay devices can alter protection logic or conceal faults. Such attacks undermine grid stability, compromise data integrity, and may trigger cascading failures, all while complicating attribution due to the trusted status of the puppet nodes. Attackers can specifically use puppet devices to flood the network with attack packets by taking advantage of flaws in protocols like dynamic source routing. This will overload the communication bandwidth and result in a DoS attack [21][23].

3.5.25. Masquerade attack

To obtain unauthorized access and commit harmful acts, an attacker may pose as authorized users, devices, or entities within a smart grid. The attacker manipulates data, issues destructive commands, and intercepts sensitive information via obtaining credentials, taking advantage of security flaws, or imitating reliable equipment like demand response systems, smart meters, control centers, or DERs. Because their actions seem to come from legitimate sources, they are able to evade authentication and security mechanisms through impersonation, endangering grid stability, causing outages, promoting financial theft, and causing infrastructure damage. To carry out these breaches, attackers use phishing, malware, social engineering, and MitM techniques, which erode confidence and make forensic investigations more difficult. For example, they pose as DERs to cause grid instability, send malicious directives from infiltrated control centers, or clone smart meters to inflate energy use. They cause false trips that activate protective relays and interfere with the distribution of power to customers by taking advantage of flaws in trusted identities and communication protocols [21–23].

3.5.26. Advanced persistent threat

With significant resources at their disposal, advanced persistent threat (APT) actors penetrate smart grid systems over time to keep an eye on and manage its cyber-physical layers. Prominent instances like Stuxnet and Industroyer demonstrate how these attackers take advantage of weaknesses and alter industrial control systems to jeopardize vital

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

infrastructure. APT organizations can disrupt operations, steal confidential information, and jeopardize grid stability by consistently accessing systems through a covert and extended presence. They employ sophisticated techniques and targeted strategies that undermine both the cyber and physical components of smart grids [21][23].

3.5.27. Adversarial machine learning attacks

Adversarial machine learning techniques craft malicious inputs to deceive machine learning models, causing them to make incorrect predictions or classifications. In smart grids, where machine learning supports critical functions such as load forecasting, anomaly and intrusion detection, energy theft identification, and grid stability monitoring, attackers exploit model vulnerabilities to trigger erroneous decisions, disrupt operations, or conceal malicious actions. They carry out evasion attacks by subtly altering data during inference to evade detection, poisoning attacks that corrupt training data to implant false behaviors or backdoors, and model inversion or extraction attacks that repeatedly query models to extract sensitive information. Trojan (backdoor) attacks embed hidden triggers that activate malicious behaviors under specific conditions. These attacks infiltrate through compromised smart meters, communication networks, cloud analytics platforms, or open-source machine learning tools. Their consequences include operational disruptions, financial losses from energy theft, privacy breaches, and erosion of trust in AI systems. For example, research shows that small perturbations can mislead load forecasting neural networks, evasion attacks can reduce detection accuracy by half in SCADA intrusion detection systems, and poisoned updates in FL can degrade global model performance. Such manipulations, especially targeting anomaly detection, critically threaten the integrity of the smart grid's cyber layer [23].

3.5.28. Grid balancing attacks

Adversaries target smart electrical grids by launching grid balancing attacks that disrupt demand response and frequency stability, utilizing various cyberattack techniques, including deception cyberattacks, DoS attacks, delay attacks, and replay attacks. These attackers manipulate the fragile real-time balance between electricity supply and demand by interfering with generation, load, or control signals, which destabilizes frequency and voltage, triggers protective shutdowns, and causes cascading failures or widespread blackouts. By compromising digital communication and automated control systems, they deceive grid operators into taking inappropriate balancing actions, thereby threatening the reliability, safety, and economic stability of smart grids [107].

3.5.29. Vulnerabilities in network communication protocols

Smart grids integrate digital communication and control systems into traditional power networks, enabling utilities and consumers to communicate with each other in a bidirectional manner. However, many communication protocols they depend on, such as DNP3, Modbus, IEC 60870-5-104, and IEC 61850, prioritize reliability and real-time performance over cybersecurity. These legacy protocols lack encryption and authentication, leaving them vulnerable to spoofing, replay, and MitM attacks. For instance, attackers can intercept DNP3 communications to inject false commands that disrupt power delivery or exploit devices supporting both secure and insecure protocol versions (e.g., IEC 61850 with TLS and plaintext) by forcing them to downgrade to insecure modes, which facilitates eavesdropping and manipulation. Furthermore, the weak security of wireless protocols used by smart meters grants attackers easy access to critical grid data [55][98].

3.5.30. Malware attack

Malware poses a threat to smart grids and virtual power plants by infiltrating their interconnected devices and control systems. Attackers deploy malicious software, such as trojans, worms, spyware, and ransomware, to gain unauthorized access, disrupt operations, manipulate data, and steal sensitive information. By exploiting vulnerabilities in ICS and SCADA networks, malware rapidly spreads across the grid, causing operational disruptions, physical damage, and large-scale outages [55][98][108-110].

3.5.31. Ransomware attack

Ransomware encrypts critical data and system files within smart grid infrastructures, blocking access until victims pay a ransom—usually demanded in cryptocurrency. Attackers infiltrate these grids by sending phishing emails, exploiting unpatched vulnerabilities in SCADA or ICS systems, compromising IoT devices with weak credentials, abusing remote access tools, or launching supply chain attacks through infected software updates. Once inside, ransomware spreads laterally, encrypts essential files, including control system data, and displays ransom demands with threats of increased payments or data leaks. Disrupting real-time monitoring, control functions, and communication systems causes operational downtime, loss of grid visibility, delayed incident response, financial losses, and endangers public safety. To evade detection, ransomware disguises its activities, maintains persistence via registry modifications or legitimate processes, and sometimes steals sensitive data before encryption. High-profile attacks, such as the shutdown of the Colonial Pipeline and assaults on utilities in Michigan and South Africa, highlight the devastating impact of

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

ransomware on critical energy infrastructure and emphasize the urgent need to strengthen cybersecurity defenses in smart grids [104][108].

3.5.32. Session hijacking

Session hijacking is a cyberattack technique where attackers seize control of active communication sessions between systems, posing significant security risks to smart grids. These grids rely on secure, continuous, and real-time data exchanges among devices, including smart meters, control centers, substations, and DERs. By intercepting or predicting authentication tokens, session IDs, or other communication identifiers, attackers impersonate legitimate participants to access sensitive systems or data without authorization. They exploit vulnerabilities like weak encryption, poor key management, session token reuse, weak authentication protocols, and insecure APIs or channels. The most common methods include TCP/IP hijacking, MitM attacks, and session theft via malware or cross-site scripting in smart grid portals. When attackers hijack sessions, they manipulate meter readings to steal energy, alter demand-response commands to disrupt load balancing, or turn off security features to disconnect substations or interfere with DER integration. These attacks cause operational disruptions, financial losses, consumer distrust, and regulatory penalties. For instance, attackers have impersonated smart meters to falsify consumption data, commandeered SCADA sessions to trip circuit breakers, manipulated demand-response events, and exploited insecure public Wi-Fi to hijack sessions. Ultimately, session hijacking enables intruders to take control of authorized nodes and utilize those sessions to issue unauthorized commands or extract sensitive information [103].

3.5.33. Supply chain attack

Adversaries compromise software, hardware, or services during manufacturing or distribution to infiltrate smart grid infrastructure, targeting trusted third parties instead of launching direct cyberattacks. By integrating ICT with traditional power systems, smart grids increase digital connectivity and broaden the attack surface, making supply chains vulnerable entry points. These attackers employ stealthy, persistent tactics, such as malicious firmware updates, compromised vendors, counterfeit hardware, and insecure subcontractors, to target specific utilities or cause widespread disruption. High-profile incidents, such as the SolarWinds breach, Ukrainian grid firmware attacks, allegations against Supermicro motherboards, and vulnerabilities in smart meters, underscore the potential for supply chain compromises to disrupt operations, facilitate espionage, and erode trust. Attackers introduce backdoors in hardware or software, risking systemic failures, data theft, and manipulation of demand-response mechanisms. Physical threats, including stolen infrastructure components and geopolitical shortages of critical materials, further strain grid security and reliability. As smart grids expand digital controls, insider threats, and emerging cyber-physical risks also increase. In response, nations focus on securing supply chains and establish trusted partnerships to protect the evolving smart grid ecosystem against growing cyber and physical threats [103][106].

3.5.34. Physical security threats

In smart grids, unauthorized individuals physically accessing critical infrastructure, devices, or components tamper with hardware, cause damage, or install rogue devices to disrupt operations and enable cyberattacks. Attackers manipulate smart meters, RTUs, and PMUs to alter data or inject malicious firmware, sabotage transformers and substations to cause outages, steal portable devices containing sensitive credentials, or exploit insider access to bypass security controls. These actions disrupt operations, compromise data integrity, trigger cascading failures, create safety hazards, and open pathways for broader cyber intrusions. Furthermore, attackers target the supply chain by embedding vulnerabilities during the manufacturing or distribution of hardware and software, underscoring the need for rigorous vendor vetting and verification. The widespread integration of IoT devices increases vulnerability, as attackers exploit inadequate security in these components to penetrate critical systems [55][77][98].

3.5.35. False pricing attacks

False pricing attacks pose a significant cybersecurity threat to smart grids by allowing attackers to manipulate energy price signals and disrupt market operations. Exploiting the communication infrastructure behind dynamic or real-time pricing, attackers inject fraudulent signals, replay outdated prices, intercept and alter data, or spoof price broadcasts to deceive consumers and producers. By fabricating false prices, they trigger sudden load shifts as demand response participants adjust their consumption, causing grid overloads, instability, and economic losses. For instance, attackers may inject artificially low prices during peak hours to induce demand surges, suppress local prices to manipulate decentralized markets, or replay off-peak prices at peak times to provoke unintended demand spikes. These tactics destabilize the grid, undermine market fairness, and erode consumer trust. Meanwhile, grid operators must continually update prices based on consumption patterns, but attackers strive to alter this pricing within their resource constraints, forcing operators to allocate defensive resources strategically to protect pricing information and maintain system stability [111].

3.5.36. Flooding attack

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Attackers carry out flooding attacks in smart grids by overwhelming communication channels, network nodes, or control systems with large volumes of illegitimate traffic, exhausting critical resources such as CPU, bandwidth, and storage, and disrupting legitimate operations. These attacks manifest as DoS attacks targeting specific components, such as smart meters; DDoS attacks that utilize multiple compromised devices to flood networks, such as the AMI; protocol-based floods that exploit communication weaknesses, like TCP SYN floods; and application-layer floods that imitate legitimate user requests to overload grid management systems. Flooding attacks increase message delays and drain energy by forcing devices to boost transmission power through malware, thereby reducing the availability, reliability, and responsiveness of smart grid applications. This disruption can cause delayed control responses, loss of real-time grid visibility, financial damage, and safety hazards. For instance, the 2015 Ukrainian power grid attack demonstrated how flooding and network disruptions can facilitate coordinated cyberattacks by concealing malicious activity and hindering recovery efforts. Overall, flooding attacks degrade smart grid performance by consuming vital resources, breaking end-to-end connections, and blocking the timely delivery of legitimate messages, ultimately threatening grid stability and security [22][88].

3.5.37. Social engineering

Social engineering, a non-technical cyber threat that exploits human psychology rather than system vulnerabilities, poses a critical risk to smart grids—complex networks that combine traditional power infrastructure with ICTs. Attackers exploit the increasing interconnectivity and reliance on both human and automated decisions by targeting utility employees, vendors, consumers, and third-party providers, who often serve as the weakest links in cybersecurity. Using deception, persuasion, and impersonation, they compromise the confidentiality, integrity, and availability of grid operations through tactics such as phishing (especially spear phishing), pretexting, baiting, quid pro quo, and physical methods like tailgating. For example, attackers send spear phishing emails disguised as critical software updates, impersonate IT staff to steal login credentials, or leave infected USB drives with enticing labels to trick employees into deploying malware. These attacks can disrupt SCADA systems, trigger power outages, damage infrastructure, steal sensitive consumer data, and destabilize demand response systems by creating artificial energy fluctuations, thereby disrupting the balance of energy supply and demand. Additionally, compromised vendors may introduce malware or faulty components via the supply chain. High-profile incidents, such as the Dragonfly 2.0 campaign and the Ukraine power grid attacks, illustrate how social engineering enables attackers to infiltrate critical energy infrastructure and cause widespread disruption [22].

3.5.38. Phishing attacks

Phishing attacks threaten smart grid ecosystems by exploiting human vulnerabilities to breach the confidentiality, integrity, and availability of critical infrastructure. Attackers deceive utility employees, contractors, system administrators, and even automated interfaces using spoofed emails, fake websites, malicious attachments, and impersonation of trusted personnel to target operational and IT components such as SCADA systems, smart meters, and IoT devices. Through techniques such as spear phishing, whaling, clone phishing, and phishing via IoT portals, they steal credentials, disrupt operations, manipulate data, and cause service outages, as seen in real-world incidents, including the 2015 Ukraine power grid attack, as well as simulated campaigns at the Idaho National Laboratory. Because smart grids heavily depend on human-machine interaction and remote access, they remain particularly vulnerable, especially during periods of operational stress. These attacks not only compromise system security but also threaten sensitive customer data and regulatory compliance, underscoring the urgent need for continuous vigilance and proactive defense measures [55][100][102].

3.5.39. Zero-day vulnerabilities

Zero-day vulnerabilities are undisclosed flaws in software or hardware that attackers exploit before vendors release patches to address them. In smart grids, these vulnerabilities pose significant risks by targeting the integration of digital communication, sensors, and control systems with critical infrastructure and legacy technologies. Attackers leverage zero-days to disrupt grid operations, cause power outages, manipulate smart meter billing, create IoT botnets, falsify real-time data from measurement units, and intercept control signals through compromised communication protocols. High-profile attacks, such as Stuxnet, TRITON, and Dragonfly 2.0, as well as exploits targeting smart meters, illustrate how attackers utilize zero-day vulnerabilities to manipulate industrial processes, compromise safety systems, and steal sensitive information, thereby threatening both infrastructure integrity and national security [55].

3.5.40. Wormhole attack

Wormhole attacks pose a significant threat to wireless ad hoc and sensor networks, which are crucial for smart grid communications. In these attacks, malicious nodes collaborate to form a low-latency “wormhole tunnel” that links distant network segments. By capturing packets at one point and rapidly tunneling them to another, the attackers deceive legitimate devices into perceiving false neighbors or shorter routes, rerouting traffic through the wormhole. This manipulation disrupts routing, enables data interception and alteration, injects false information, and facilitates

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

DoS attacks. In smart grid components such as AMI, SCADA systems, and PMUs, wormhole attacks can cause communication delays, inaccurate billing, compromised load balancing, and distorted topology data. For instance, attackers near smart meters and utility servers intercept and replay meter data, corrupting the utilities' information. As mobile ad hoc networks gain prominence in smart grids, their limited resources and deployment conditions increase their vulnerability to wormhole attacks, endangering the availability and integrity of critical grid operations [22].

3.5.41. Covert attack

Attackers carry out covert attacks on smart grids by secretly altering system inputs to manipulate outputs without detection, posing one of the most sophisticated threats to grid security. They leverage detailed knowledge of the grid's protocols, system models, and device architectures to inject malicious code and remain hidden for extended periods. Known as closed-loop replay attacks, these covert operations seamlessly mimic normal activity, allowing attackers to cause subtle yet persistent disruptions such as FDI, load redistributions, topology changes, or replayed measurements [22].

3.5.42. Load drop attacks

In smart grids, adversaries carry out load drop attacks by manipulating metering infrastructure like the AMI to send service disconnect commands to consumer smart meters, causing sudden drops in power demand. By exploiting vulnerabilities in smart meters, HEMS, or IoT devices, attackers remotely disrupt or falsify consumption data, prompting the grid to misinterpret demand and adjust generation incorrectly. These actions destabilize the power system, potentially causing shutdowns, power quality violations, and abnormal operations, while inflicting economic and operational damage [22].

3.5.43. Smart meter tampering

Smart meters are essential to smart grids, enabling two-way communication between utilities and consumers, collecting detailed energy usage data, supporting dynamic pricing, and improving grid management and fault detection. However, their connectivity and decentralized design make them vulnerable to cyber threats, particularly tampering. Attackers deliberately manipulate meter hardware or software to disrupt normal operations by altering consumption data, disabling communication, or injecting malicious commands into the grid network. They tamper with meters for personal gain, such as stealing electricity, causing disruptions, or launching broader cyber-physical attacks. Methods include physically bypassing sensors, placing magnets to distort measurements, cutting power, modifying firmware, exploiting software vulnerabilities to change settings, erase logs, or turn off tamper detection, and intercepting or spoofing communication data to deceive utilities. These attacks result in economic losses for utilities, threaten grid stability, compromise consumer privacy, and create entry points for more extensive cyberattacks. Real-world examples, such as the Puerto Rico fraud case (2009–2012), firmware vulnerabilities in Spain (2015), and hacking incidents in India (2022), demonstrate the persistent and evolving nature of these risks [23].

4. CYBER SECURITY IN SMART GRID

Smart grids modernize traditional power systems by integrating advanced communication, automation, and information technologies to enhance the efficiency, reliability, and sustainability of electricity production and distribution. However, this digital transformation increases the connectivity and interdependence between physical and cyber components, creating significant cybersecurity challenges. To protect smart grids, organizations must safeguard data confidentiality, integrity, and availability while implementing strong authentication, authorization, and non-repudiation measures. They should design tailored cybersecurity strategies that secure both digital and physical assets, protect customer information, and minimize the risks of cyberattacks. Adopting a proactive, adaptive, and collaborative approach aligned with international standards and robust architecture is essential. Key actions include encrypting data, enforcing access controls, monitoring network activity, and fortifying defenses. Organizations must engage with the National Institute of Standards and Technology (NIST) interoperability framework, establish sound governance, identify critical assets, and conduct regular risk assessments. Implementing a comprehensive incident response plan enables rapid detection, mitigation, and recovery from cyber threats [102]. By thoroughly understanding and applying these security requirements, stakeholders ensure system stability, protect consumer data, and maintain a reliable electricity delivery system. Below are some of the security requirements in the smart grid.

4.1. Confidentiality

Smart grids protect sensitive information, such as user consumption data, control commands, and grid status, by preventing unauthorized access and disclosure. Because smart grids rely on real-time, bidirectional communication, maintaining confidentiality is crucial to avoid privacy breaches, data manipulation, and cyberattacks. They restrict access to consumer information (including energy usage, billing details, and personal identity), operational data (such as control commands and status updates), and communications among control centers, substations, field devices, and

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

smart meters. With the increasing internet connectivity of home appliances, safeguarding customer data, especially billing and usage information, has become even more critical. To preserve data integrity and shield personal and proprietary information, smart grids employ encryption methods such as ECC and homomorphic encryption, enforce strong authentication and access control systems, including attribute-based encryption, and adopt secure communication protocols designed to protect privacy in resource-constrained devices, like smart meters and home networks [21][112].

4.2. Integrity

Smart grids rely on integrity as a fundamental security requirement to ensure data accuracy, consistency, and integrity throughout the transmission, storage, and processing processes. As these grids increasingly exchange real-time data across interconnected digital systems, they face growing threats from integrity attacks, such as FDI, message tampering, and unauthorized modifications, which can lead to incorrect control actions, billing errors, and operational disruptions. Such attacks may manipulate customer data, device statuses, or voltage readings, undermining grid reliability. To defend against these threats, researchers design lightweight cryptographic protocols, including prekeying mechanisms and aggregation schemes, that protect critical communications within strict resource and timing limits. Blockchain-based frameworks further enhance integrity by employing decentralized ledgers and smart contracts to automate access control and create tamper-proof records. Resilience is further increased by adaptive, decentralized defenses against cyber-physical threats offered by multi-agent and machine learning-driven anomaly detection systems. Secure data sharing, real-time control, and maintaining the credibility of contemporary smart grids as they adjust to future energy demands all depend on maintaining strong integrity procedures [21][113][114].

4.3. Availability

To guarantee consistent and dependable access to energy services and grid operations, irrespective of cyber threats or system malfunctions, availability is a crucial security need in smart grids. Attacks, particularly DDoS attacks, are more likely to occur as IoT devices and advanced communication technologies become more integrated. These attacks have the potential to interrupt information flow and cause widespread outages or operational breakdowns [21]. Smart grid systems use redundancy, strong network designs, and real-time monitoring to promptly identify and minimize interruptions to guarantee availability. By facilitating quick threat identification and response, emerging technologies like AI, blockchain, and software-defined networking improve grid resilience [21]. By detecting and eliminating threats that evade basic defenses, intrusion detection and prevention systems (IDPS) offer a crucial secondary defense [115]. Additionally, availability ensures that when needed, authorized users may consistently access vital components like dispersed control centers, SCADA, and DMS. Any outage can have serious repercussions for the economy and society since the smart grid serves essential industries [116].

4.4. Authentication

Authentication plays a vital role in smart grids by ensuring that only authorized users and devices can access and interact with the grid infrastructure, thereby preventing unauthorized access, impersonation, and various cyberattacks. Modern authentication schemes address challenges such as limited device resources, real-time communication requirements, and the need to preserve user privacy. Researchers have developed advanced protocols that leverage ECC and lightweight cryptographic operations to achieve mutual authentication, anonymity, and resistance to threats such as key compromise, impersonation, replay, and MitM attacks, all while minimizing computational and communication overhead [112][117]. Some approaches incorporate quantum key distribution (QKD) and edge computing to guarantee unconditional security, especially in smart metering systems [118]. Meanwhile, blockchain-based authentication protocols decentralize trust, enhancing the reliability and auditability of authentication processes. By confirming the identities of communicating parties, securing data transmission, and preventing adversaries from impersonating legitimate users or providers, robust authentication mechanisms safeguard smart grids [116].

4.5. Authorization and access control

Authorization and access control are essential for ensuring that only legitimate users and devices access sensitive data and resources within smart grids. These mechanisms protect the confidentiality, integrity, and availability of grid operations by blocking unauthorized access, preventing data breaches, and stopping malicious activities. After authenticating a user or device, the system enforces authorization policies that limit access and operations based on predefined privilege levels. Based on user identity and pertinent regulations, access permissions are assigned by Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC). Security frameworks usually use permission to control access to resources after authentication as the first line of protection. Attackers can remotely control circuit breakers or RTUs and deliver destructive commands, destroying

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

portions of the network or the entire system, if they get past authorization in SCADA systems. Additionally, authorization systems allow users to access particular data, guaranteeing that the availability of data corresponds with the permissions that have been granted [113][119].

4.6. Non-repudiation

A safe basis for trust is provided by non-repudiation in smart grids, which guarantees that all participants to communications or transactions cannot retract their actions, such as transmitting messages or carrying out directives. This security feature holds users, devices, and service providers responsible for their behavior, preventing conflicts over invoicing, control signals, and energy usage. Non-repudiation builds trust, promotes audits, settles disputes, and makes forensic analysis easier since smart grids depend on real-time, bidirectional data interchange between components like smart meters, sensors, RTUs, and SCADA systems. Verifiable, tamper-proof communication is made possible by cryptographic methods like blockchain, public key infrastructure (PKI), hash functions, and digital signatures. For instance, a smart meter uses its private key to digitally sign consumption data, enabling the utility company to confirm the data's accuracy and authenticity. By preserving unchangeable, traceable transaction records, blockchain improves accountability. Modern methods like QKD offer complete protection against repudiation, guaranteeing that data transfers are reliable and verifiable. Along with providing legal documentation to satisfy regulatory standards, these methods also identify criminal actions, including energy theft, false meter reporting, insider threats, and illegal commands. The dependability and credibility of smart grid activities are enhanced by non-repudiation [120].

4.7. Accountability

In smart grids, accountability entails tracking, documenting, and monitoring user and device behavior to determine who is accountable for security lapses or policy infractions. Smart grids encounter difficulties including privacy breaches, malevolent activity, and uncontrollable entities as they depend more and more on distributed architectures and real-time data sharing. Accountability frameworks utilize protocols to stop key misuse and enable responsibility tracking, enforce multi-authority control using attribute-based encryption, and put in place systems that trace and attribute data access or modifications in order to mitigate these risks. By leveraging blockchain and smart contracts, these frameworks ensure transparent, auditable data sharing, while integrating authentication and authorization systems to permit only authorized actions and log all activities for review. Together, these features strengthen the security, transparency, and trustworthiness of smart grid operations, promote regulatory compliance, and boost user confidence. Beyond the three core NIST security criteria, accountability acts as a vital safeguard by making all actions traceable, clarifying responsibilities, and maintaining comprehensive system records. For instance, smart meters in households provide detailed consumption and billing data; however, attacks targeting smaller service providers can cause inconsistencies that weaken overall accountability [121].

4.8. Anonymity

Anonymity is crucial for securing smart grids by protecting users' identities and blocking unauthorized access to sensitive consumption data that can reveal personal behaviors, such as household occupancy and appliance use. Since smart meters continuously exchange fine-grained energy data with utility providers, smart grids employ robust anonymity techniques to prevent profiling, surveillance, and targeted attacks. These techniques include pseudonymization, mix networks, anonymizing networks, homomorphic encryption, differential privacy, group and ring signatures, and lightweight cryptographic protocols, which obscure identities, unlink data from individuals, and enable secure, privacy-preserving data analysis and authentication. Advanced methods, such as identity-based aggregate signatures and designated verifier protocols, validate data without revealing user identities. Meanwhile, conditional anonymity enables trusted entities to trace identities under regulated conditions, thereby striking a balance between privacy and security oversight. By integrating these approaches, smart grids secure communications and data sharing, foster user trust, and ensure compliance with privacy regulations [117].

4.9. Untraceability

Untraceability plays a crucial role in securing smart grids by protecting user privacy and preventing the association of identities, consumption patterns, and communication behaviors with specific individuals or devices. Since smart grids continuously collect and transmit detailed data, such as real-time energy usage, appliance activity, and user schedules, they require robust untraceability mechanisms to stop adversaries, including service providers and insiders, from inferring sensitive information, launching targeted attacks, or conducting surveillance. To achieve this, smart grids

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

employ advanced cryptographic and anonymity-preserving techniques, including pseudonymization, anonymous credentials, mix networks, onion routing, private information retrieval, homomorphic encryption, and differential privacy. They also employ lightweight authentication protocols and enhanced key agreement schemes to secure unlinkable communications across sessions, while privacy-preserving traffic signaling hides the origin of consumption data to maintain confidentiality. Although untraceability enhances privacy, smart grid systems must strike a balance with accountability and operational requirements; therefore, many adopt conditional untraceability, which permits authorized entities to revoke anonymity under strict legal or policy conditions in cases of fraud, disputes, or emergencies [112][117][122].

4.10. Attacks resilience

Smart grids demonstrate attack resilience by resisting, tolerating, and recovering from cyber and physical attacks while maintaining performance and service continuity. As interconnected cyber-physical systems, they integrate traditional power infrastructure with advanced communication, control, and information technologies to enable real-time monitoring, demand response, and distributed energy management. However, this integration broadens the attack surface and exposes new vulnerabilities across all domains. To ensure resilience, smart grids implement layered defenses that include secure design, strong authentication, encryption, regular updates, real-time anomaly detection, swift isolation of compromised components, fail-safe mode switching, and rapid recovery through redundancy and automated reconfiguration. Researchers enhance these capabilities with machine learning-based intrusion detection, adaptive control, decentralized multi-agent defenses, event-triggered consensus algorithms, and cyber-physical risk modeling to counter threats like FDI, DoS, and coordinated attacks. Innovations such as blockchain for tamper-proof logging, secure multiparty computation for collaborative decision-making, and self-healing architectures further bolster resilience. By embedding these strategies across devices, networks, and control centers, smart grids secure, stabilize, and reliably deliver energy amid evolving cyber threats [117][123].

4.11. Session key negotiation

Session key negotiation secures smart grid communications by enabling entities, such as smart meters, control centers, and service providers, to exchange trusted, confidential, and authenticated data. After mutual authentication, this process establishes a temporary secret cryptographic key that encrypts and verifies all data during a session. Because smart grids operate in dynamic, distributed, and resource-constrained environments, key negotiation protocols must remain efficient, lightweight, and resilient to cyber threats like impersonation, replay, and MitM attacks. Researchers commonly employ cryptographic techniques such as Elliptic Curve Diffie–Hellman (ECDH), identity-based cryptography (IBC), and PKI, often enhancing protocols with features like mutual authentication, forward and backward secrecy, key freshness, and resistance to key compromise impersonation. Innovations, including ECC-based schemes, two-round key exchanges, hybrid encryption using fuzzy extractors, and PKI-free designs, reduce overhead while maintaining robust security. Some advanced protocols also protect user privacy through anonymity and untraceability. As smart grid systems evolve, researchers develop lightweight, quantum-resilient key negotiation methods to ensure data confidentiality, integrity, and overall system trustworthiness [112][117].

5. FEDERATED LEARNING IN SMART GRIDS

FL is a groundbreaking approach that protects data privacy while allowing several clients to work together to train machine learning models across decentralized data sources [124]. Client agents without sharing raw data train models locally on their devices or servers, as explained by Shalan et al. [30], Wang et al. [125], and Khan [126]. The training procedure is managed by a centralized server, which never has direct access to the client data. A decentralized substitute for conventional centralized training, FL was first presented by Google in 2016 and addresses privacy issues while lowering network load. This method involves clients sending only updated model parameters, not raw data, to the central server and doing local training on their datasets during each training round. These parameters are then combined by the server to produce a global model, which is then sent back to the clients. While retaining all training data on their devices, this iterative

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

loop allows customers to improve their local models in light of the updated global model. According to Orabi et al. [37] and Wang et al. [125], FL improves privacy protection and minimizes network traffic by sending only model parameters. Until the model reaches a desired accuracy or finishes a predefined number of rounds, the process is repeated [127].

FL protects sensitive data during exchange and transfer while optimizing client devices' processing resources. A central server initializes a global model at the beginning of the process and chooses clients according to their processing and storage capabilities. Each client receives the initial model and its parameters, trains the model locally using its own data, and computes updates, like weight changes or gradients. These updates return to the server, which aggregates them—commonly using Federated Averaging (FedAvg)—to update the global model. This cycle of client selection, local training, update transmission, and aggregation repeats over multiple rounds until the global model converges, as detailed by Orabi et al. [37], Liu et al. [128], and Elshazly et al. [129]. Fig. 7 illustrates the processes involved in FL.

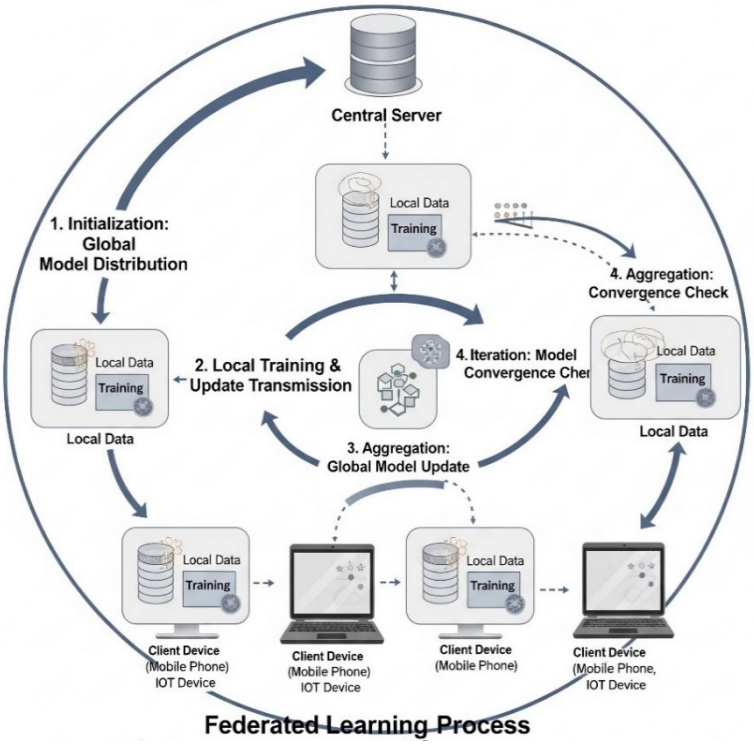

Fig. 7. Illustrates the processes involved in FL.

FL operates on three core principles that collectively enhance privacy and model performance. First, each node retains its local data on-site, reducing the risk of data breaches common in centralized systems and eliminating the need for the server to handle raw data during training. Second, nodes collaboratively train a shared predictive model by performing local computations and sending only model updates, such as gradients or weights, to the central FL server. This server aggregates these updates to produce an improved global model, which it then distributes back to the nodes, enabling the system to adapt effectively in dynamic environments such as smart grids. Third, the server iteratively refines the global model by continuously collecting updates from nodes, redistributing the refined model for further local training, and repeating this process until the model achieves satisfactory accuracy [130]. FL preserves privacy by keeping raw data securely on local devices, while enabling decentralized and distributed training across multiple clients simultaneously. It supports both synchronous and asynchronous training, and it effectively manages heterogeneous, non-identically distributed, and imbalanced data across participants. Unlike distributed learning, which centralizes data before processing, FL transmits only secured model parameters, often protected by perturbation and encryption, during communication. By coordinating numerous remote devices working on independent datasets—potentially differing from the global distribution—FL enables

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

participants to collectively reach model accuracy close to that of a fully centralized system with complete data access [131-133].

FL frameworks classify data distributions into three types: horizontal, vertical, and federated transfer learning. Horizontal FL involves parties with datasets sharing the same features but different samples, who train models locally and share only updates with a central server. This setup maintains privacy through secure multi-party computation, homomorphic encryption, and differential privacy, ensuring sensitive data remains on local devices [127][134]. Vertical FL facilitates collaboration among organizations holding different feature sets for the same user base. Organizations securely align user samples using Private Set Intersection protocols to combine features and collaboratively train a model without sharing raw data. This approach improves accuracy while ensuring compliance with regulations such as GDPR and the Health Insurance Portability and Accountability Act (HIPAA) [111][112][135]. Federated transfer learning combines federated and transfer learning to handle heterogeneous feature spaces, label spaces, and data distributions, enabling knowledge transfer across clients with limited or unaligned data. It employs cryptographic techniques to safeguard privacy and minimize computational costs, thereby supporting cross-domain learning in low-data environments [37][136].

In smart grid applications, FL enables consumers and devices to train local models using their own data and send only model updates to a central server, which aggregates them into a refined global model, thereby preserving privacy. This decentralized training enhances renewable energy forecasting, fault detection, optimal power flow, load forecasting, and the detection of electricity theft. FL reduces communication overhead through optimization algorithms such as Federated Averaging (FedAvg) and more advanced methods like FedProx, QFedAvg, and FedOptim, which address device heterogeneity, fairness, and efficiency. Additional strategies, such as asynchronous communication, device subsampling, and fault tolerance, mitigate challenges arising from varying device capabilities. Innovations such as edge-cloud collaboration further support privacy-preserving data sharing and incentivize participation, positioning FL as a robust, scalable alternative to traditional centralized machine learning in privacy-sensitive domains like smart grids, healthcare, finance, and IoT [137-139].

5.1. Applications for Federated Learning in Smart Grids

Some of the applications of FL in smart grids include the following:

5.1.1. Load forecasting

Load forecasting predicts future electricity demand across various time horizons, ensuring the stability and efficiency of the smart grid. Traditional centralized methods face issues with privacy, scalability, and cybersecurity due to the extensive data collection required. FL overcomes these challenges by training models locally on devices, such as smart meters, and sharing only encrypted updates with a central server. This approach preserves privacy, distributes computation, and enhances scalability. Researchers use models such as long short-term memory networks to capture temporal consumption patterns, convolutional neural networks (CNNs) to identify spatial patterns in geographically distributed grids, gradient boosted decision trees to handle structured tabular data with high accuracy, and support vector regression to provide a robust baseline for smaller datasets within federated frameworks to capture complex consumption patterns. Applications range from household load prediction to grid stability and demand response strategies [28][140][141].

5.1.2. Adaptive learning

In smart grids, adaptive learning enables the system to dynamically adjust to changing data, user behaviors, and environmental conditions, thereby managing the grid's complexity and decentralization. FL supports this by enabling devices, such as smart meters, HEMS, EVs, and DERs, to train models locally and share only updates, not raw data, with a central server. This decentralized approach lowers communication load, increases scalability, and protects data privacy. Each node's model updates help the global model adapt to diverse scenarios in real time. FL also improves bandwidth efficiency and ensures resilience against communication or node failures. These benefits make it ideal for adaptive learning in smart grids [130][141].

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

5.1.3. Resilience to data poisoning

FL enhances smart grid defenses against data poisoning by decentralizing model training across multiple edge devices, thereby limiting the impact of compromised nodes. It employs robust aggregation methods, such as Krum and Trimmed Mean, to filter out poisoned updates and assigns trust scores to down-weight suspicious clients. The central aggregator detects anomalies with machine learning, while differential privacy and gradient clipping reduce manipulated updates. Cross-validation from redundant data and adversarial training further enhances resilience. These techniques protect key functions such as load forecasting and fault detection. By preserving privacy and enabling scalable continuous learning, FL ensures model integrity and grid reliability against attacks [130][142][143].

5.1.4. Scalable and efficient response to cyber threats

FL enables smart grid components, such as smart meters, substations, and EV charging stations, to collaboratively train machine learning models locally for intrusion detection and threat classification. Each node processes its own cybersecurity data and sends encrypted updates to a central aggregator, which integrates them into a global model. This approach supports scalable, platform-independent learning across diverse devices, from resource-limited edge nodes to complex control centers. By continuously updating models in real time, FL enhances threat detection and system resilience. It preserves data privacy, complies with regulations like GDPR and NIS2, and resists targeted attacks through its decentralized design. As the grid grows, FL seamlessly incorporates new devices, ensuring adaptive and robust cybersecurity [28][130][144].

5.1.5. Collaborative defense mechanisms

FL empowers grid components, such as substations, smart meters, and EV chargers, to collaboratively detect and respond to threats without sharing raw data. Each node trains local anomaly models and shares only parameters to build a global defense model, enabling real-time updates and peer-to-peer coordination. Trust mechanisms help weigh contributions, enhancing resilience against coordinated attacks. This decentralized collaboration enhances threat detection accuracy and enables operators to proactively mitigate risks across the grid [28][130].

5.1.6. Anomaly and intrusion detection

Advanced digital communication and control technologies have enhanced the efficiency and flexibility of smart grids, but also increased their vulnerability to cyber threats, including data tampering, DoS attacks, FDI, and unauthorized access. Traditional centralized intrusion detection systems face challenges such as high latency, limited scalability, privacy issues, and single points of failure. To address these issues, researchers now utilize FL, which enables smart meters, substations, and DERs to collaboratively train global models without sharing raw data, thereby preserving privacy. By using local data from distributed grid components, FL detects cyber threats early, from unauthorized access to coordinated DDoS attacks. This decentralized approach enhances scalability, privacy, and fault tolerance, while tailoring detection models to diverse grid environments. Consequently, it strengthens smart grids' resilience against evolving cyber threats [134][145][146].

5.1.7. Energy trading and market optimization

Modern smart grids optimize energy trading by balancing supply and demand, integrating DERs, and maximizing economic efficiency. Centralized methods struggle with issues such as privacy, data heterogeneity, latency, scalability, and security. FL addresses these challenges by enabling consumers, producers, and utilities to collaboratively train models locally without sharing raw data, thereby preserving privacy and enhancing security. It shares only model updates, cutting communication costs and scaling efficiently across many participants. This decentralized approach also enhances system resilience by eliminating single points of failure. For instance, prosumers in local energy communities jointly train forecasting models on their data, share parameters with a central aggregator, and improve trading, revenue, and grid stability [147][148].

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

5.1.8. Demand response management

Demand response management is crucial in smart grids, enabling utilities to adjust electricity demand in response to supply fluctuations using price incentives or direct control. Traditional systems rely on centralized data processing, but they face challenges related to privacy, scalability, communication, and security. FL addresses these issues by letting smart meters train local models on private data and share only updates with a central server. This approach enhances privacy, reduces communication latency, and improves scalability. It supports decentralized load forecasting, personalized demand response, real-time optimization, and privacy-preserving energy scheduling. Recent studies and pilots confirm the potential of FL to revolutionize demand response while complying with data protection regulations [112][132][149][150].

5.1.9. Predictive maintenance of grid equipment

In smart grids, predictive maintenance anticipates equipment failures to minimize downtime, reduce costs, and enhance reliability. FL protects privacy and makes real-time analytics possible by allowing grid nodes, such as substations, transformers, and sensors, to train models locally using their own data. Nodes share model updates with a central aggregator, which refines and redistributes a global model for additional training, rather than sending raw data. This approach scales with the decentralized nature of the grid, combines many datasets, and securely manages sensitive data. It regularly updates local models to identify problems in real time, like insulation problems or overheating. Federated predictive maintenance improves grid resilience, accuracy, and efficiency through iterative model improvement [151].

5.1.10. Renewable energy forecasting

By facilitating cooperative model training without necessitating the exchange of raw data, FL improves renewable energy forecasts in smart grids. Only updates are sent to a central aggregator by each DER, such as wind turbines or solar panels, which trains local models using its own private data. By combining these updates into a global model, the aggregator reduces communication traffic, preserves privacy, and increases accuracy. This decentralized approach increases robustness, facilitates continuous learning with fresh data, and supports a variety of DER networks. By integrating FL, operators can increase the integration of renewable energy, lower costs, and improve grid reliability. In the end, it promotes robust and sustainable energy systems [112][148][152].

5.1.11. Electric vehicle charging optimization

FL is revolutionizing EV charging optimization in smart grids by enabling EVs, charging stations, and grid operators to collaboratively train predictive models without sharing sensitive data. This decentralized approach protects privacy, reduces communication overhead, and ensures compliance with regulations. Frameworks like Block-FeDL secure model aggregation and validation, improving forecasting accuracy. Federated reinforcement learning methods, such as FedSAC, optimize charging and discharging in real-time, balancing grid stability and user preferences. Integrating blockchain enhances transparency in vehicle-to-everything (V2X) energy trading, while edge computing with federated deep learning facilitates low-latency, scalable, and secure V2G scheduling. These solutions enhance forecasting, load control, and economic efficiency, thereby advancing the integration of sustainable EVs [147][153][154].

5.1.12. Smart home energy management

Smart home energy management systems optimize energy consumption, enhance comfort, and integrate renewable energy sources by utilizing sensors, smart meters, and connected devices to monitor and control household energy use. Large-scale deployment raises concerns about privacy, security, and scalability. FL tackles these issues by enabling each home to train local models on its data and share only model updates with a central aggregator. This process preserves privacy, reduces communication, and supports scalability while allowing personalized tuning. Embedded in smart homes, FL improves consumption forecasting, appliance scheduling, demand response, and renewable integration without compromising user

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

confidentiality. Consequently, it offers smart grids a secure, efficient, and scalable solution that enhances user empowerment and grid sustainability [112][155][156].

5.1.13. Grid stability and frequency control

Frequency stability is crucial for the reliable operation of power systems, as deviations from the nominal 50 or 60 Hz can damage equipment and trigger power outages. Traditional centralized controls manage frequency by collecting data from generators, loads, and storage devices. However, the rise of DERs, such as rooftop solar, wind turbines, and electric vehicles, introduces variability and complexity that challenge these conventional methods. FL enables DERs and grid nodes to collaboratively train models on local data without sharing sensitive information. This decentralized approach improves frequency control by preserving privacy, reducing communication load, and adapting to real-time grid changes. Consequently, smart grids can deploy advanced predictive controls that enhance frequency stability, integrate renewable energy sources, and improve grid resilience [44][157][158].

5.2. Security and Privacy Challenges in Federated Learning

Despite its promising benefits, FL faces several critical hurdles that must be addressed to ensure its secure and efficient operation. These security and privacy challenges across multiple aspects of the FL framework highlight the need for robust solutions to support its widespread adoption. Below are the detailed descriptions of the security and privacy challenges in FL.

5.2.1. Poisoning attacks

Poisoning attacks in FL involve malicious clients injecting manipulated data or tampering with model updates to corrupt the global model. These attacks fall into two main categories: data poisoning, where adversaries introduce mislabeled or biased samples into their local datasets (e.g., label flipping or backdoor triggers), and model poisoning, where attackers directly alter update vectors before sending them to the central server (e.g., scaling, directional, or optimization-based attacks). These methods exploit the FL system's decentralized nature, limited client-side observability, and inherent data heterogeneity. Attackers may pursue various objectives, including targeted misclassification, general performance degradation, system destabilization, or the injection of harmful biases. The persistent threat of poisoning undermines the integrity, robustness, and trustworthiness of FL systems [9][36][135][159].

5.2.2. Byzantine failures

In FL, Byzantine failures pose a serious security and privacy threat by allowing clients, or in rare cases, the central server, to behave arbitrarily or maliciously during training. Originating from the Byzantine Generals Problem, these failures involve sending misleading or corrupted updates that degrade model performance, prevent convergence, or leak private data. Unlike simple faults such as crashes or network issues, Byzantine clients act strategically to poison the global model, perform data or model inversion attacks, and evade detection. These failures can result from compromised devices, buggy software, or adversaries exploiting vulnerabilities. Common attack strategies include model poisoning (e.g., uploading scaled, flipped, or backdoored gradients), data poisoning (e.g., training on mislabeled data), Sybil attacks (where one adversary controls multiple clients), and free riding (submitting outdated or random updates). The consequences are severe, including degraded model accuracy, unstable or failed convergence, privacy breaches, and erosion of trust in FL systems, particularly in critical domains like energy [9][111][133][135].

5.2.3. Sybil attacks

In FL, a Sybil attack poses a significant threat, where a malicious actor creates numerous fake clients (Sybil nodes) to exert excessive influence over the training process. These Sybil clients participate in FL rounds and submit carefully crafted updates that poison the global model, degrade performance, insert backdoors for specific misclassifications, or extract private data from honest clients through adversarial updates. Even with client sampling strategies, the attacker's chances of selection remain high due to the volume of fake identities. Sybil attacks compromise model integrity, system reliability, and client privacy, while posing

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

detection challenges due to the client anonymity inherent in FL and the natural diversity of legitimate client updates. As a result, they severely undermine the fairness, security, and trustworthiness of FL systems [135].

5.2.4. Communication attacks

Communication attacks in FL exploit insecure transmission channels to intercept, manipulate, or disrupt model updates exchanged between clients and the server. Since FL depends on periodic updates, such as gradients or weights, attackers can target these to compromise the integrity, confidentiality, or availability of the training process. The common threats include MitM attacks, where adversaries intercept and alter updates to eavesdrop on private data, inject malicious gradients, or delay convergence; eavesdropping and inference attacks, which passively or actively extract sensitive information such as private data samples or membership status from gradients; and poisoning attacks that inject adversarial updates, leading to backdoors or degraded performance through label flipping or gradient manipulation. Attackers may also forge packets or tamper with transmissions, undermining trust and spreading misinformation. Meanwhile, DoS and jamming attacks can block communication altogether, particularly in edge or mobile FL environments. These vulnerabilities intensify in the absence of secure protocols (e.g., Secure Sockets Layer/Transport Layer Security), unauthenticated participants, limited device resources for encryption, and network conditions such as high latency or packet loss that conceal malicious actions [36].

5.2.5. Inference attacks

Property inference attacks and membership inference attacks pose significant privacy threats in FL, where individual clients train local models on sensitive data and share updates with a central aggregator. In property inference attacks, adversaries analyze model updates, such as gradients or weights, to infer latent or unintended statistical properties of the training data, like demographic attributes or behavioral patterns. These attacks exploit the data-dependent nature of model updates and side-channel information leakage. In contrast, membership inference attacks aim to determine whether specific data instances were part of a model's training set by analyzing model responses, such as prediction confidence or loss values. In FL, attackers may observe updates to build shadow models and train classifiers that distinguish between member and non-member data. These attacks are especially potent when models are overfitted, the data is non-independent and identically distributed across clients, updates are fine-grained, or the number of communication rounds is high. Without robust defenses, such as differential privacy or secure aggregation, these vulnerabilities can compromise data confidentiality, enable profiling or discrimination, and breach regulations like the GDPR or HIPAA. As FL gains traction in privacy-sensitive domains, addressing these threats remains critical to preserving user trust and ensuring regulatory compliance [9][135][160].

5.2.6. Gradient/update leakage

Gradient or update leakage refers to a privacy threat in FL, where adversaries, such as a central server or external observers, attempt to reconstruct or infer sensitive information (e.g., images, text, medical records) from the gradients or parameter updates shared by clients. Although FL retains raw data on local devices, gradients often encode information about the underlying data, especially when clients train deep models on small or uniquely distributed datasets. Since gradients reflect how the model adjusts to specific data during training, attackers who access these updates can exploit their mathematical relationship to the original inputs. Several factors influence leakage risk: smaller batch sizes (particularly size=1) heighten the risk by tightly linking gradients to individual samples; deep models like CNNs and transformers tend to encode more information in gradients; sparse or compressed updates (e.g., top-k selection) may reduce leakage but can impact performance; and more communication rounds increase exposure. This vulnerability has profound privacy implications, including the potential reconstruction of raw data, membership inference attacks that can identify whether specific data was used in training, and attribute inference, which reveals sensitive characteristics such as race or health status. Even subtle gradient updates can expose private information, underlining the need for stronger privacy safeguards in FL [135].

5.2.7. Client profiling

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

In FL, client profiling occurs when an adversary, either internal (such as a malicious server or participant) or external, infers sensitive information about clients from the updates or metadata they contribute during the training process. Instead of reconstructing raw data, the adversary builds detailed client profiles that may reveal demographics (e.g., age, gender, location), preferences (e.g., app usage, visited websites), behavioral traits (e.g., typing speed, browsing habits), or device characteristics. Although FL keeps data local, it still exposes gradients, weight updates, and metadata that can leak information. Adversaries can exploit several vectors: they may analyze gradients or model updates to identify patterns tied to non-independent and identically distributed client data, examine communication metadata (e.g., update timing or frequency) to infer user behavior, or use model inversion attacks informed by auxiliary data to deduce client attributes. These profiling risks can lead to loss of anonymity, exposure of sensitive attributes, discriminatory targeting, and a breakdown of user trust in FL's privacy guarantees [141][161][162].

5.2.8. Trojan attack

A Trojan attack in FL occurs when a malicious client, or group of clients, intentionally injects hidden, harmful behavior into the global model during training. These attacks aim to make the model perform normally on standard inputs while producing attacker-controlled outputs in response to specific trigger inputs. Characterized by their stealthiness, Trojan attacks often evade detection since the backdoor activates only under rare conditions. Unlike random noise attacks, they cause highly targeted misclassifications, such as labeling a stop sign with a sticker as a speed limit sign. These attacks are model-agnostic and can target any architecture compatible with the FL setup. Defending against them is challenging due to limited access to client data, vulnerabilities in standard aggregation methods such as FedAvg, and the assumption that most clients are honest—an assumption that can be exploited by coordinated malicious clients. As FL gains traction, particularly in applications such as electricity theft detection in smart grids, the need for robust, privacy-preserving defenses becomes increasingly critical. Current FL-based approaches often assume trustworthy participants, which is unrealistic in practice [137], leaving the system exposed to such covert threats.

5.2.9. Lack of incentive mechanisms

Conventional FL systems often lack effective incentive mechanisms, focusing primarily on data collection and model aggregation. This setup may work in self-organized environments where data providers are under the organizer's control, but it falls short in real-world scenarios that require contributions from external participants. Without proper incentives, it becomes difficult to attract and retain valuable data providers. To address this, researchers have explored incentive mechanisms, such as deep reinforcement learning and Stackelberg Game models, to motivate participation. FL often assumes that devices willingly contribute data, but this assumption rarely holds in practice. Without effective incentives, participants may lose motivation, or worse, receive rewards without contributing, resulting in unfair compensation and degraded system performance. The absence of a robust incentive mechanism not only limits performance but also introduces security and privacy risks by encouraging dishonest behavior and reducing engagement from trustworthy contributors. A sustainable solution requires integrating cryptography, game theory, reputation systems, and fairness in machine learning to align individual incentives with collective system goals [111].

5.2.10. Single point of failure

Traditional FL architectures rely on a centralized server for model aggregation, which introduces significant vulnerabilities, including a single point of failure. In this setup, participants send their local model updates to a central aggregator, which then applies a predefined aggregation algorithm to update the global model. After aggregation, participants must download the updated global model. As the number of participants increases, the server experiences heavy network traffic and processing demands, resulting in performance bottlenecks. Suppose the central server fails or becomes compromised. In that case, the entire FL system is at risk—either through complete system failure or through unpredictable and potentially malicious behavior that could result in private data leaks. Moreover, the centralized server is vulnerable to malicious updates, which can compromise the global model and diminish the accuracy of local updates. Excessive simultaneous transmissions from local devices can also overload the network, further impacting performance

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[9][36][111]. To address these challenges, FL systems must adopt mechanisms that eliminate single points of failure and enable auditing of the aggregator's behavior.

5.2.11. Model inversion attacks

A significant challenge in FL is the risk of sensitive information leakage from local training data through shared model updates. Attackers can exploit inference techniques, such as gradient inversion or model inversion, to indirectly extract confidential details by analyzing shared parameters, including gradients, weights, or activations, during the training or inference process. These inference attacks enable adversaries to reconstruct class representatives or even individual data points without direct access to the original datasets [135][159].

5.2.12. Free-riding attacks

In FL, where participants provide computational resources and data without direct financial compensation, free riding poses a significant challenge. Some participants may contribute minimal or no resources while still benefiting from the improved global model. This behavior distorts the training process by introducing incomplete or suboptimal data, ultimately reducing the model's accuracy and performance. Moreover, the presence of free riders can discourage meaningful contributions from other participants, thereby undermining the overall efficiency of the system [159].

5.2.13. Malicious server

Adversaries can hack the FL server and turn it hostile by selectively choosing local updates from specific clients, censoring or favoring them—which unfairly disadvantages honest clients. Attackers can also cause the server to malfunction, disrupting the entire FL process. Although FL minimizes centralized data storage, the server responsible for aggregating updates remains a critical vulnerability. If compromised, it can extract sensitive information from the collected model updates [9][135].

5.2.14. Malicious client and data

Malicious or compromised clients can impact the global model by submitting fabricated data, even if the aggregator itself remains secure. Although researchers have proposed mechanisms to detect these malicious clients, these methods increase system load because they rely on an additional model to verify the authenticity of the data [111].

5.2.15. Adversarial model updates

Adversarial clients in FL send manipulated updates to compromise the global model's performance or leak data during the aggregation process. Because FL relies on collaboration between clients and the server, attackers exploit vulnerabilities in the client-server architecture and training process to launch these attacks [135].

5.2.16. Backdoor attacks

Adversaries embed hidden vulnerabilities, known as backdoors, into the global model by introducing triggers within model updates. These triggers cause the model to behave undesirably under specific conditions while allowing it to perform normally in all other situations [135]. To address these issues, researchers have widely applied blockchain technology in FL due to its tamper-resistance, anonymity, and traceability. By integrating blockchain, participants ensure transparency and maintain the integrity of model updates shared throughout the FL process. This approach also enables distributed data storage and effectively defends against model attacks from malicious entities [77][159][163].

6. BLOCKCHAIN IN SMART GRID

In 2008, Satoshi Nakamoto introduced blockchain as the foundation for Bitcoin, a decentralized digital currency that enables direct peer-to-peer transactions without relying on major financial institutions. While

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Nakamoto's implementation brought blockchain into the spotlight, the idea of a distributed ledger date back to the 1990s. At that time, Haber and Stornetta proposed a time-stamping system for digital documents, laying the groundwork for blockchain technology [164]. Since then, blockchain has undergone significant evolution and garnered increasing interest across a broad range of fields. As a decentralized and distributed ledger technology, blockchain securely records transactions across multiple nodes, eliminating the need for a central authority [32][37][139][165][166]. It maintains a shared, cryptographically linked record of transactions in "blocks," which form a continuous “chain” distributed across the network. Blockchain’s peer-to-peer architecture distributes computing power and resources among all participating nodes. This design enhances system reliability, redundancy, and overall performance. By replicating data across multiple writer nodes, the network reduces its dependence on any single authority and enhances trust and resilience against disruptions [167-169]. Each block contains a cryptographic hash of the previous block, which enforces a strict chronological order and ensures immutability through timestamping. Altering a single block would require modifying all subsequent blocks task rendered computationally infeasible by the cryptographic structure [30][133][166][170][171]. The system also incorporates Merkle Trees to compress and verify transaction data efficiently using recursive hashing. When nodes broadcast transactions, the network timestamps and validates them by solving a cryptographic puzzle that meets a specific hash requirement. This consensus mechanism ensures the ledger's security and integrity. To further improve efficiency, blockchain supports Simplified Payment Verification (SPV), which allows lightweight clients to verify transactions using only block headers. This feature reduces storage and computational overhead, particularly as the number of transactions increases [30][133][166][170][171].

Each block stores encrypted data generated through irreversible hashing algorithms. It includes information about the sender, recipient, transaction details, and timestamp [37]. By embedding the hash of the previous block's header, the blockchain forms a tamper-evident chain. Any attempt to alter a block changes its hash and invalidates all subsequent hashes. The network quickly detects and rejects such tampering, thereby preserving data integrity and transparency. As illustrated in Fig. 8, this architecture, featuring interlinked blocks and Merkle trees, enables scalable, secure, and verifiable record-keeping in decentralized systems [172].

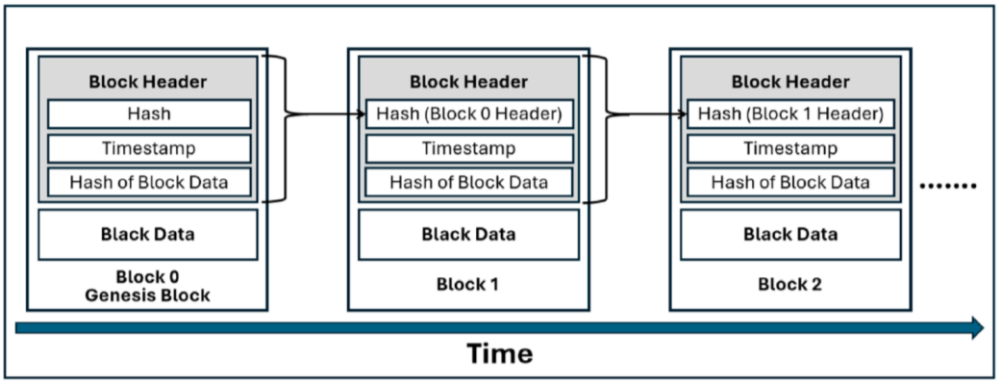

Fig. 8. Shows a general blockchain structure, where each block contains a hash from the previous block [172].

Blockchain operates as a decentralized system that eliminates the need for a central authority by relying on network nodes—or peers—to validate each new block through a consensus mechanism. This process ensures that all participants agree on the current state of the ledger. Several consensus algorithms govern how nodes reach agreement, including Proof of Work (PoW), Proof of Stake (PoS), Proof of Burn (PoB), Proof of Elapsed Time (PoET), Proof of Authority (PoA), and Practical Byzantine Fault Tolerance (PBFT). For instance, PoW requires miners to solve complex mathematical problems using significant computational power, while PoS selects validators based on their token holdings. PoB improves selection chances by requiring coin burning, PoET ensures fairness through randomized wait times, PoA relies on verified identities, and PBFT supports consensus among known participants even with a limited number of faulty nodes. The advantages and disadvantages of these algorithms differ: PoS improves scalability and energy

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

efficiency, while PoW provides strong security but uses a lot of energy. Additional optimizations are offered by variants like Proof of Activity, Leased PoS, and Delegated PoS. Nodes disseminate transactions throughout the network when users start them. Miners then gather valid transactions, propose blocks, and use the consensus mechanism to determine which block to finalize and append to the chain, ensuring consistency across all nodes.

Smart contracts further extend blockchain's capabilities by automating agreements through predefined conditions, thereby reducing the need for intermediaries and enhancing transparency. Blockchain's tamper-resistant structure builds trust by linking blocks through cryptographic hashes, forming an immutable chain that protects data integrity [172][173]. Each block contains a header with metadata, such as a timestamp, the previous block's hash, the Merkle root of transactions, and a difficulty target in PoW systems, and a body storing validated transactions in a Merkle tree. This structure supports secure, efficient, and verifiable record-keeping. A nonce in PoW systems adjusts mining difficulty, balancing network security with computational feasibility. The genesis block serves as the foundation of the chain, with each new block referencing its predecessor [165]. Blockchain systems are categorized into four types: public, private, consortium, and hybrid. Public blockchains, which usually employ PoW or PoS and permit unfettered participation, though they may give rise to privacy concerns [133][166][174]. Private blockchains provide improved performance and confidentiality by limiting access to approved users. While hybrid blockchains include public and private elements, enabling both protected activities and selective openness [174], consortium blockchains, which are controlled by chosen entities, achieve a balance between decentralization and control [166][174].

The main principles of blockchain include

- Immutability: Once data is recorded on the blockchain, changing or deleting it becomes extremely difficult. Cryptographic hashes are used to time-stamp transactions and connect them to earlier records, guaranteeing data integrity and guarding against fraud and manipulation. Because of its immutability, blockchain is a reliable and long-lasting network that improves historical accuracy and traceability. The distributed network of nodes that underpins blockchain innovation ensures that any recorded transaction stays unchanged, making the ledger extremely reliable and impenetrable to tampering [133][175][176].
- Decentralization: A central authority, like a bank or government, is not required to validate transactions because blockchain works on a decentralized network of computers, or nodes. Through the reduction of single points of failure and the promotion of peer-to-peer interactions, this decentralized structure improves system resilience. Because every node keeps a complete copy of the blockchain ledger, no one entity can take control of the entire network. The system is more resistant to fraud and tampering because of this architecture [11][133][175][176].
- Transparency: All transactions are recorded on public blockchains in a way that is transparent to all users, and network consensus is required for any modifications. This transparency promotes accountability, increases user trust, and makes auditability easier. Particularly in public blockchains like Bitcoin and Ethereum, each node may independently ensure that blocks stay unchanged and verify the accuracy of the data, resulting in a highly transparent ecosystem [133][176].
- Distributed ledger: The blockchain ledger, which contains all transaction records, is shared across all nodes in the network. This distribution ensures that every participant has access to the same source of truth, thereby improving data availability and redundancy. By reducing reliance on centralized databases, the distributed ledger enables rapid observation of changes and requires every node to participate in validation and maintenance of the ledger [175].
- Cryptographic security: Blockchain employs advanced cryptographic techniques to secure data privacy, authenticity, and integrity. It uses hash functions (e.g., SHA-256) to generate unique digital fingerprints, public-key cryptography for identity and transaction signatures, and digital signatures for authentication and non-repudiation. Each record is individually encrypted, increasing overall network security [175][176].

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

- Consensus mechanisms: To validate and agree on the ledger's state, blockchain uses consensus algorithms such as PoW, PoS, Delegated PoS (DPoS), and PBFT. These mechanisms ensure that all distributed participants reach a consensus, prevent double-spending, and defend the network against specific attacks, such as Sybil attacks. Consensus enables nodes to make rapid, impartial decisions, ensuring the system functions reliably even when nodes do not trust one another [175].
- Traceability: Blockchain enables tracking and tracing of all transactional data across the network, enhancing accountability and transparency. Because all transactions remain permanently recorded, authorized nodes can retrieve complete historical information at any time [133].
- Auditability: Every transaction on the blockchain is recorded with a digital time-stamp and validated on the distributed ledger. Network participants can audit and trace transactions freely, promoting transparency in token flows and operations [111][133].
- Smart contracts: Smart contracts are self-executing programs that automatically enforce coded rules and agreements when predefined conditions are met. They reduce reliance on intermediaries, automate workflows, and increase operational efficiency while minimizing human error.
- Tokenization and incentives: Blockchains represent value, assets, or rights using digital tokens, which incentivize participants to act honestly and contribute resources such as computing power. This system supports new economic models, such as token economies, which encourage engagement in decentralized ecosystems, including decentralized finance (DeFi) and non-fungible tokens (NFTs).
- Persistency: Because blockchain links blocks through one-way hash functions, modifying any recorded information requires altering all subsequent blocks—a computationally infeasible task. The distributed nature of the system ensures that participants verify block validity, enabling the network to quickly detect and counter falsification attempts. This design renders blockchain tamper-proof and immutable [111][133].
- Programmability and extensibility: Blockchain platforms, such as Ethereum, enable the development of decentralized applications (dApps) and new protocols, fostering innovation across various industries. They support decentralized governance, autonomous organizations (DAOs), and flexible system designs. Programming smart contracts enables automation of complex corporate processes, reducing the need for intermediaries [169].
- Resiliency: The decentralized design of blockchain eliminates single points of failure, making the network robust and resilient to faults. All nodes store the whole blockchain, enabling quick detection and correction of errors or malicious activities [169].
- Anonymity and pseudonymity: Users interact through cryptographic addresses rather than personal information, preserving privacy while maintaining transaction traceability. This balance supports transparency and confidentiality but presents regulatory and compliance challenges [111][133].

Blockchain technology fortifies data integrity and security by leveraging its inherent immutability to prevent unauthorized modifications, making it particularly effective for securing logs, forensic evidence, and system backups. It empowers users through self-sovereign identities and automates access control using smart contracts, which enhance authentication and decentralized identity management. In IoT and secure communications, blockchain plays a crucial role by registering devices, validating data exchanges, and safeguarding firmware updates against tampering. Its decentralized architecture mitigates DDoS attacks by supporting resilient DNS and traffic verification, while also improving software development through secure code tracking and transparent audit trails. Blockchain enables the secure and incentivized sharing of cyber threat intelligence, ensures the cryptographic integrity of transactions, and streamlines compliance by automating the logging of user actions. By decentralizing certificate authorities, it replaces traditional PKI systems, manages certificate issuance and revocation transparently, and verifies digital signatures without relying on intermediaries. Furthermore, it combats counterfeiting and enforces digital rights via content authenticity checks, license control, and distribution tracing [173][174].

Blockchain also enhances incident response by time-stamping events, preserving immutable custody chains, and enabling collaborative efforts across agencies. In power systems and IoT environments, it securely records tamper-proof data on energy usage and transactions, eliminating single points of failure and

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

improving resilience against cyberattacks. Privacy-preserving techniques, such as zero-knowledge proofs, protect sensitive data, while smart contracts automate IoT processes, reduce operational errors, and enhance overall efficiency. These contracts also enforce tamper-proof access control, enable real-time auditing, and support dynamic, transparent access policies. By distributing control and decentralizing authority, blockchain fosters a secure, transparent, and resilient foundation for smart grids and IT infrastructures. It enables real-time anomaly detection and addresses conventional security vulnerabilities through a trustless, decentralized approach [30][176][177].

6.1. Blockchain for Secure Federated Learning in Smart Grids

FL in smart grids faces significant security and trust challenges due to data heterogeneity, adversarial participants, and the absence of a central, trusted authority. Blockchain technology addresses these issues by providing a decentralized, tamper-proof, and auditable infrastructure that enhances the security, integrity, and trustworthiness of FL operations. In this blockchain-enabled framework, edge devices, such as smart meters, act as local clients, training models using private data on energy consumption or generation. By working together to develop a common global model without sharing raw data, these devices protect privacy and cut down on communication overhead. Without depending on a central server, a decentralized blockchain ledger safely logs all model updates and transactions, guaranteeing transparency and data integrity. Consensus techniques, like PBFT or PoS, verify these changes and preserve network uniformity. Important tasks, including model aggregation, incentive distribution, reputation management, and access control, are automated by smart contracts. Sensitive grid data is further protected by sophisticated privacy techniques such as secure multi-party computation, homomorphic encryption, and differential privacy.

A central coordinator or the blockchain network initiates the training process by establishing the global model architecture and allocating initial parameters to participating edge nodes as the first step in the workflow for blockchain-secured FL in smart grids. Every node uses its own private data to train the model locally before sending the model updates to the blockchain as transactions. These updates are verified by the consensus mechanism and recorded on the immutable ledger by nodes in the blockchain network. The verified updates are subsequently safely combined into a new global model using smart contracts or decentralized aggregation techniques. This updated model is broadcast back to all nodes, allowing them to refine their local models in subsequent iterations. Smart contracts also manage the incentive and reputation systems, rewarding valid contributions and discouraging malicious or low-quality behavior. The process repeats until the model converges or reaches the desired level of performance, ensuring transparent, secure, and efficient collaborative learning [35-37][139]. Fig. 9 illustrates the workflow for blockchain-secured FL in smart grids.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

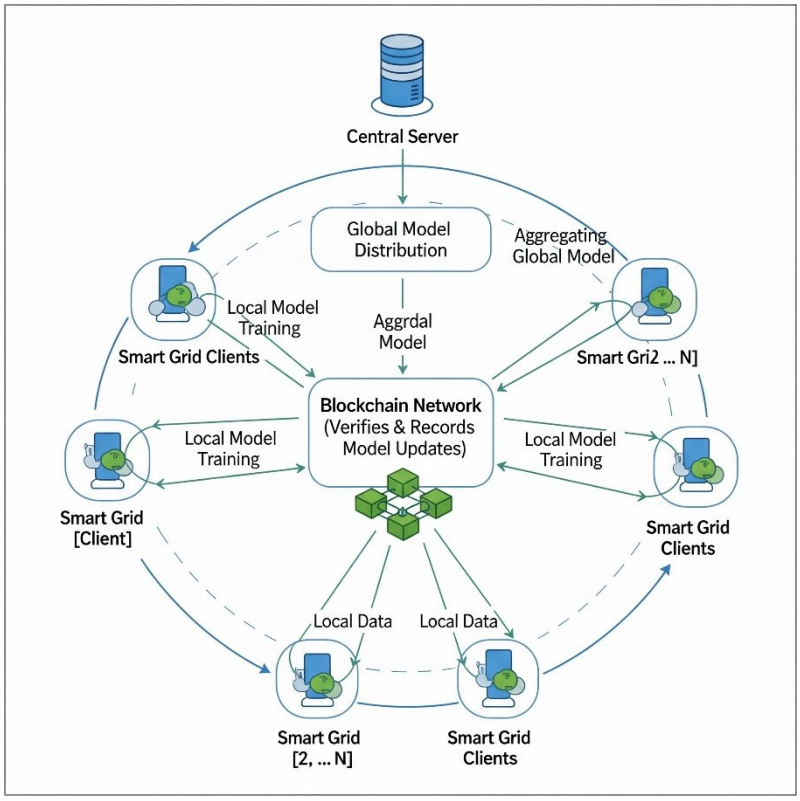

Fig. 9. Illustrates the workflow for blockchain-secured FL in smart grids.

By replacing the central server with a peer-to-peer blockchain network, this approach mitigates vulnerabilities inherent in traditional FL architectures. It eliminates single points of failure and defends against threats like model poisoning, data inference, and update manipulation. Blockchain enables distributed validation and aggregation of model updates, with each transaction immutably recorded for complete transparency and accountability. Smart contracts enforce update rules, verify formats, and manage participation timelines, while consensus algorithms prevent unauthorized alterations. Reputation systems and token-based incentives foster fairness and discourage malicious behavior. Blockchain also supports decentralized identity verification, role-based access control, and immutable audit trails, strengthening privacy and system governance. Furthermore, it coordinates secure computation methods such as zero-knowledge proofs and secure multi-party computation, ensuring both data confidentiality and model accuracy. These capabilities position BFL as a secure, scalable, and ethically robust framework for collaborative AI, with proven impact across smart grids [34-37].

6.2. Benefits of Blockchain in Federated Learning for Smart Grids

Blockchain significantly enhances FL by addressing key challenges in privacy, security, trust, and decentralization, especially in critical domains such as smart grids. By eliminating centralized aggregators, blockchain enables secure, decentralized model training while keeping raw data local. It leverages smart contracts to enforce privacy-preserving data usage policies, manage access control, and automate incentive distribution based on participant contributions. Immutable ledgers ensure auditability, transparency, and regulatory compliance by recording all model updates and transactions. Consensus mechanisms such as proof-of-validation verify the integrity of model updates, defending against poisoning attacks and malicious contributions. Blockchain supports secure model aggregation, traceable decision-making, and decentralized governance, strengthening trust and system reliability in multi-stakeholder environments [34][37][133]. BFL forms a closed-loop system that promotes trusted collaboration and resilient energy management. It creates dedicated ledgers and global model state trees to securely track weight updates during training iterations. It improves participation through token- or reputation-based incentive mechanisms and ensures

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

fairness by penalizing abnormal behavior. Technologies like homomorphic encryption and IPFS further enhance privacy and storage efficiency. BFL also fosters interoperability across heterogeneous systems by providing standardized protocols and secure cross-organizational collaboration. While scalability and complexity remain ongoing challenges, BFL offers a robust, incentive-driven architecture that enables near real-time model updates, distributed control, and regulatory adherence—paving the way for autonomous and privacy-preserving intelligent systems [133][178].

6.3. Limitations and Trade-offs of Blockchain in FL for Smart Grids

Below are the detailed descriptions of the limitations and trade-offs of integrating blockchain in FL for smart grids:

- Communication and computation overhead: Integrating blockchain into FL for smart grids introduces significant communication and computation overhead. Writing each local update from clients, such as smart meters or substations, to the blockchain adds latency, slowing down training rounds. The execution of smart contracts for verification, consensus, and model updates also demands considerable computational resources. Moreover, since many nodes store the entire blockchain ledger, they propagate redundant data that may be of little relevance to local decision-making. These factors create trade-offs between security and efficiency. While blockchain enhances auditability and trust, it also increases resource utilization and training time. Similarly, although transparency promotes accountability, maintaining an immutable, replicated ledger can hinder scalability as the number of participants grows.
- Scalability challenges: Because of the blockchain's ongoing expansion and the transaction throughput's limitations, scalability is still a major problem in BFL. There are difficulties for real-time FL operations since platforms like Ethereum can only handle a certain number of transactions per second. Edge devices' storage capacities are strained as a result of handling an increasing amount of data as FL activity grows. Developers are forced under these circumstances to balance performance and decentralization. Although a highly decentralized system improves resilience and trust, responsiveness is frequently sacrificed. Furthermore, lowering the blockchain's update frequency can ease network congestion, but it may also slow model convergence and lower overall accuracy.
- Energy consumption: In energy-conscious settings like smart grids, the high energy consumption of blockchain—especially when combined with PoW consensus mechanisms—presents significant difficulties. There is a trade-off between security and sustainability because most edge devices lack the processing power and energy capacity to execute complex blockchain computations. More power is needed for stronger consensus protocols, even when they improve security. Restricting participation to only capable nodes can enhance system performance, but it also weakens network resiliency and inclusivity by reducing decentralization and excluding less powerful devices.
- Data privacy and confidentiality: The immutability of blockchain frequently clashes with privacy laws like GDPR, which require data erasure. Sensitive information may still be exposed by on-chain metadata even if raw data remains off-chain. Transparency and privacy are traded off as a result of these conflicts. Blockchain can decrease user anonymity if it is not combined with robust privacy-preserving safeguards, even as it facilitates auditability and traceability. Developers must carefully strike a balance between openness, privacy protection, and regulatory compliance in smart grids, where data confidentiality is essential.
- Consensus protocol suitability: Finding the right consensus mechanism is essential to balancing scalability, efficiency, and security. PoW is inefficient and energy-intensive, yet it provides good security. PoS is vulnerable in some situations and raises centralization problems. While other protocols, such as PBFT, have reduced latency, they have trouble scaling when there are a lot of nodes. Although they can speed up model changes, lightweight consensus techniques may compromise security. Although a more decentralized strategy lowers presumptions about trust, it also makes the system more complex, which makes maintenance and deployment more difficult.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

- Interoperability and standardization: Blockchain and FL integration in smart grids is made more difficult by a lack of standards and interoperability. Compatibility problems across platforms arise from the variety of devices and communication methods. In the absence of widely recognized guidelines for incorporating BFL, developers must choose between portability and customization. Although they might work effectively for certain grid configurations, custom solutions hinder interoperability. Furthermore, although advantageous, the rapid speed of blockchain innovation runs the danger of system fragmentation and makes large-scale deployments more difficult.
- Security and expanded attack surface: By adding additional risks like smart contract vulnerabilities, Sybil attacks, and 51% attacks, integrating blockchain into FL increases the attack surface of the system. The added complexity increases the likelihood of misconfigurations, including insecure nodes, keys, or access controls. Although blockchain enhances security through transparency and traceability, it does not eliminate all risks. Public blockchains, lacking identity-linking mechanisms, make it challenging to trace malicious clients. Sharing training data or metadata on-chain can expose sensitive information and lead to privacy leakage. Openness promotes collaboration but also increases potential entry points for adversaries, requiring organizations to implement robust security management practices and carefully balance security with system complexity [111].
- Economic and incentive design: Designing fair and effective incentive mechanisms is particularly difficult in environments where monetary rewards are impractical. Token-based incentives may encourage participation but also introduce speculation and volatility. Poorly designed incentive structures are vulnerable to exploitation. Reputation systems, although valuable for building trust, may also be manipulated, leading to unfair exclusion. Developers must carefully balance motivation and fairness, considering factors such as data quality, contribution volume, and participation frequency.
- Training efficiency: Beyond model accuracy, training efficiency is a key metric in practical FL systems. Blockchain integration can reduce efficiency because high latency delays processes, particularly when clients are located in different geographical locations. In untrusted networks, verifying data consumes a considerable amount of time, further slowing down operations. Moreover, some frameworks use cryptographic tools, such as zero-knowledge proofs and homomorphic encryption, which are computationally intensive and slow in their current implementations. These inefficiencies can render BFL impractical in specific contexts [111].
- Incentive mechanism limitations: While cryptocurrencies like Bitcoin and Ethereum demonstrate successful blockchain-based payment systems, applying similar incentive models in FL is challenging due to resource constraints. FL environments cannot afford the computational expense of PoW. Incentive mechanisms must consider multiple factors, such as the amount and quality of data contributed, participation frequency, and client reliability. These considerations are highly sensitive and require carefully designed algorithms [111].
- General integration challenges: Despite its benefits, integrating blockchain with FL in resource-constrained environments introduces persistent challenges, including transaction speed, scalability, and energy consumption. As the number of participants and model updates increases, the blockchain risks congestion, slowing down the training process. Consensus protocols like PoW are computationally heavy and unsuitable for lightweight devices. Additionally, the growing size of blockchain can overwhelm devices with limited storage capacity. Blockchain's transparency may also conflict with the privacy requirements of FL. To address these issues, researchers are exploring lightweight consensus mechanisms, off-chain solutions, sharding, and privacy-preserving techniques to improve performance and reduce overhead [37].
- Computational inefficiencies and confidentiality risks: Although BFL frameworks support decentralized model aggregation, they often incur high computational costs and pose confidentiality risks. The blockchain's public nature, while promoting transparency, can compromise privacy. These trade-offs highlight the need for further innovations in secure, scalable, and efficient blockchain-FL systems [9].

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Integrating blockchain with federated learning in smart grids involves significant limitations and trade-offs. To overcome these challenges and ensure long-term security against quantum attacks, system designers must adopt PQC while making careful design decisions.

7. POST-QUANTUM CRYPTOGRAPHY IN SMART GRID

Quantum computers threaten the security of traditional asymmetric cryptographic algorithms, such as RSA and ECC, by enabling powerful attacks through algorithms like Shor's and Grover's. These quantum algorithms can solve mathematical problems, like factoring large integers and computing discrete logarithms, exponentially faster than classical methods, making current cryptosystems vulnerable. To safeguard core principles of digital security, including confidentiality, integrity, and availability, researchers are developing PQC. Marchsreiter [179] and Attar et al. [180] define PQC, also known as quantum-resistant or quantum-safe cryptography, as cryptographic algorithms designed to secure digital communication and data against the risks posed by quantum computers, particularly in sectors such as energy that require long-term protection. As quantum computing advances, traditional keys—although secure by today's standards—may become obsolete, prompting the urgent need to transition to quantum-resistant systems [178][181][182].

To address these emerging risks, the NIST launched a global initiative to standardize PQC algorithms. After receiving 69 algorithm submissions in 2016, NIST selected four for standardization by 2022: CRYSTALS-Kyber for key encapsulation mechanisms (KEMs), and CRYSTALS-Dilithium, Falcon, and SPHINCS+ for digital signatures. The first draft standards, published in 2023, detail the performance and trade-offs of each algorithm. Alongside NIST, the Internet Engineering Task Force (IETF) standardized stateful hash-based signature algorithms—XMSS and LMS—which are now part of NIST's Special Publication 800-208. PQC algorithms fall into three main categories: public key encryption (PKE), KEMs, and signature schemes. These systems secure messages, establish shared keys, and authenticate transactions in quantum-resistant ways. PQC emphasizes backward compatibility, algorithmic diversity, and efficiency, supporting integration into current infrastructure, constrained devices, and high-throughput environments. Beyond securing today's data, PQC also protects against "harvest now, decrypt later" threats and extends to advanced primitives, such as zero-knowledge proofs [179][183][184].

Researchers categorize PQC algorithms into five primary approaches based on the mathematical problems they exploit: lattice-based, code-based, multivariate polynomial-based, hash-based, and isogeny-based cryptography [185]. Each approach offers unique principles and strengths that contribute to the broader field of quantum-resistant security. Hash-based cryptography, introduced by Ralph Merkle in the 1970s, leverages the robustness of cryptographic hash functions and underpins secure digital signatures, such as XMSS and SPHINCS+. Although these schemes offer strong security rooted in well-understood primitives, they face drawbacks such as large signature sizes and slower performance [180][181][185]; [186]. Lattice-based cryptography relies on the hardness of problems such as the Shortest Vector Problem (SVP), the Closest Vector Problem (CVP), and the Learning With Errors (LWE) problem, enabling secure and efficient primitives like CRYSTALS-Kyber and Dilithium, which NIST has selected for use. It provides a strong balance of security and performance, despite relatively large key and ciphertext sizes [180][185][186]. Code-based cryptography, rooted in the difficulty of decoding random linear codes, encompasses schemes such as Classic McEliece and HQC KEM, which offer high throughput and quantum resistance but are hindered by large key sizes and limited versatility [180][185]. Multivariate polynomial cryptography leverages the NP-hardness of solving multivariate quadratic equations, providing compact signatures and keys through schemes such as GeMSS and Rainbow (although NIST excluded Rainbow due to structural weaknesses). Despite their potential, many Multivariate polynomial cryptography schemes remain vulnerable or inefficient [180][186]. Finally, isogeny-based cryptography, which leverages the difficulty of computing isogenies between super singular elliptic curves, offers compact keys and ciphertexts ideal for constrained environments. However, it remains computationally demanding and underdeveloped, particularly after the cryptanalysis of SIKE [187][188]. Each category contributes distinct advantages and trade-offs, reflecting ongoing efforts to secure cryptographic systems against quantum threats.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

The application of PQC in smart grids focuses on enhancing the security and resilience of critical infrastructure against emerging threats posed by quantum computing. Below are brief descriptions of the applications of PQC in smart grids.

- Secure communication: Secure M2M communication is essential for smart grids, which rely on interconnected components such as sensors and smart meters. To defend against classical and quantum threats, researchers now embed PQC into protocols such as TLS, MQTT, IEC 61850, and DNP3. By replacing RSA and Diffie–Hellman with quantum-resistant algorithms, such as lattice-based cryptography, PQC ensures long-term data confidentiality and authentication. Hybrid encryption models and QKD further enhance security, even on resource-constrained platforms. As quantum computing evolves, PQC-based communication is emerging as a critical pillar for smart grid privacy, reliability, and resilience [5][38][189].
- Authentication and access control: PQC enhances authentication and access control in smart grids by utilizing quantum-resistant digital signatures, such as CRYSTALS-Dilithium and SPHINCS+. These schemes protect against spoofing, impersonation, and MitM attacks—even from quantum-capable adversaries. Researchers have designed lightweight, standards-compliant protocols for secure device communication and identity management. Advanced methods such as QKD and semi-QKD enhance the security of smart meters and sensors. Formal analyses and real-world tests confirm their scalability, efficiency, and resilience against both classical and quantum threats [39][190].
- Firmware and software integrity: Developers can protect embedded devices, such as RTUs and IEDs, from tampering by signing firmware updates with post-quantum digital signature algorithms, like lattice-based Dilithium-5. These quantum-resistant methods verify code authenticity and integrity against both classical and quantum attacks. Researchers have successfully integrated these signatures into blockchain and SCADA systems, thereby enhancing the immutability and auditability of software. Optimized implementations run efficiently on resource-constrained devices, making them suitable for smart grid environments. As cyber threats continue to grow, PQC is becoming increasingly essential for securing reliable and regulation-compliant smart grid operations [40][191].
- Privacy preservation: Smart meters generate detailed usage data that must be protected from unauthorized access. PQC ensures privacy in smart grids by replacing vulnerable algorithms, such as RSA and ECC, with quantum-resistant alternatives. Techniques such as lattice-based cryptography and homomorphic encryption secure energy consumption and billing data against classical and quantum threats. Researchers have developed efficient privacy-preserving protocols for state estimation, demand response, and data aggregation using these methods. Real-world simulations and formal analyses confirm their scalability, low overhead, and resilience to emerging quantum attacks [192-194].

By fending against quantum computer threats, PQC provides robust long-term protection, making it a workable and future-proof data security solution. Its software-based distribution across devices and cost-effectiveness make it even more appealing to businesses. PQC does, however, come with some significant difficulties. It typically relies on much larger key sizes than classical public-key algorithms, which, while improving security, significantly impact performance. PQC algorithms often require more time for encryption and decryption, consume more storage and memory, and demand higher network bandwidth. Many also struggle to maintain cryptographic hardness at scale; for instance, although lattice-based cryptography shows promise, it often achieves only average-case hardness. Additionally, PQC remains sensitive to advances in quantum computing, meaning early algorithms may need upgrades or replacements as quantum capabilities evolve [5].

7.1. Roles of Post-Quantum Cryptography in Enhancing Federated Learning within Smart Grids

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

PQC strengthens the security of FL in smart grid systems by protecting against threats from both classical and quantum adversaries. Below are the detailed descriptions of PQC's roles within FL environments of smart grids:

7.1.1. Securing model updates against quantum threats

In smart grids, FL enables distributed devices (e.g., smart meters, sensors) to train models locally and share updates with a central aggregator. Although these updates exclude raw data, they can leak sensitive information, requiring secure transmission. Quantum computers pose a threat to classical cryptography, including RSA and ECC, making model updates susceptible to attacks. PQC resists quantum attacks using lattice-, code-, or hash-based schemes. Algorithms like Dilithium and SPHINCS+ secure updates through quantum-resistant signatures and MACs. Frameworks such as PQS-BFL and Beskar integrate PQC with differential privacy and blockchain to ensure confidentiality, authenticity, and resilience in FL [42].

7.1.2. Enhancing authentication in edge devices

Edge devices in smart grids, such as smart meters and sensors, collect real-time data that supports the implementation of FL. Operating in unsecured environments, these devices are vulnerable to impersonation and data injection risks. PQC offers quantum-resistant authentication using lattice-, hash-, code-, and multivariate-based algorithms. Unlike RSA or ECC, PQC-based digital signatures resist both classical and quantum attacks, securing device identities and communications. Lightweight PQC schemes, such as Dilithium, run efficiently on constrained edge devices, enabling robust and low-overhead authentication. Integrating PQC with blockchain and secure aggregation further enhances trust, traceability, and resilience in FL processes [39][40][193].

7.1.3. Preserving long-term data privacy

In smart grids, sensors and smart meters generate sensitive data that reveal usage patterns and the state of the infrastructure. FL supports a collaborative model training approach without exposing raw data; however, local model updates can still leak private information. PQC secures these updates against both classical and quantum threats. Quantum-resistant methods, like lattice-based encryption (e.g., Kyber, NTRU), homomorphic encryption, and differential privacy, protect data and enable secure aggregation. Blockchain-integrated smart grids benefit from PQC through secure queries and proxy re-encryption. PQC-based protocols ensure long-term privacy, forward secrecy, and trust in smart grid FL [192][193][195].

7.1.4. Quantum-resilient secure aggregation

Post-quantum secure aggregation is essential for privacy-preserving, tamper-resistant FL in smart grids, protecting sensitive data from energy meters, substations, EVs, and edge controllers. Traditional cryptographic methods, such as RSA and ECC, are vulnerable to quantum attacks. Therefore, researchers are integrating lattice-based, code-based, and multivariate polynomial algorithms into protocols that resist such threats. These enhanced protocols enable homomorphic encryption and key-homomorphic pseudorandom functions, supporting efficient single-round aggregation with low communication overhead. Frameworks like Beskar combine PQC with differential privacy to defend against diverse adversaries while maintaining model accuracy. They ensure confidentiality, robustness against dropouts, and integrity despite the presence of malicious participants. By adopting these protocols, smart grid FL achieves quantum-resistant security, system resilience, and user privacy protection [41][42].

7.1.5. Strengthening federated identity management

In smart grid environments, federated identity management coordinates secure authentication, authorization, and access control across diverse entities operating under different administrative domains. To stop adversarial attacks, illegal access, and impersonation, FL needs a strong identity system. By substituting quantum-resistant signatures for weak schemes, PQC fortifies this framework and makes it possible for safe device onboarding and decentralized trust via self-sovereign models or blockchain. With short-lived certificates and compact revocation, it prevents identity theft and facilitates scalable credential management. The security of device credentials and access privileges is further improved by hybrid cryptography

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

techniques. When taken as a whole, these safeguards guarantee that only authorized parties engage in FL, protecting smart grid privacy and integrity from quantum attacks [5][39][40].

7.1.6. Protecting communication channels

Secure communication between smart meters, substations, and coordinators in FL-enabled smart grid systems protects model updates, keys, and metadata from being intercepted and altered, especially by adversaries with quantum capabilities. PQC combats these dangers by using challenging mathematical issues that are difficult for quantum computers to handle, such as lattice-based systems. PQC improves security even on resource-constrained edge devices by enabling end-to-end encryption, strong authentication, and quantum-safe key exchanges (like CRYSTALS-Kyber). Integrating PQC with protocols like TLS 1.3 and QKD further strengthens defense. NIST-approved algorithms such as Kyber, Dilithium, and FALCON are increasingly deployed to secure FL in smart grids. These technologies ensure long-term privacy, integrity, and resilience against evolving quantum threats [36][38][192].

7.1.7. Enabling blockchain-backed auditing

In FL for smart grids, integrating PQC into blockchain audit mechanisms ensures secure and transparent accountability among decentralized participants. Quantum-resistant signatures, such as Dilithium, protect model updates, metadata, and actions by logging them on a tamper-proof, quantum-secure blockchain. These signatures authenticate devices, prevent forgery, and maintain learning integrity while preserving data privacy. Combined with blockchain's immutability, they enable long-term verification, detect malicious updates, and enforce smart contracts without the need for central authorities. Multi-signature schemes and smart contracts automate validation, boosting scalability and audit efficiency with minimal overhead. This approach enhances security and traceability against both classical and quantum threats while preserving the decentralized nature of FL [40][196].

7.1.8. Facilitating robust key management

PQC secures FL in smart grids by enabling robust and scalable key management that is resistant to quantum attacks. It replaces vulnerable protocols like RSA and ECC with quantum-safe algorithms, such as lattice-based and code-based methods, that protect model updates and authenticate participants across diverse edge devices. Lightweight KEMs support efficient key negotiation, periodic rotation, and forward secrecy, even under dynamic network conditions. By organizing device groups according to function or region, hierarchical key management architectures improve scalability and make management and administration easier. Dilithium, FALCON, and SPHINCS+ are examples of standardized algorithms that offer quantum-resistant authentication and signatures. These methods provide data integrity and safe, reliable communication amongst smart grid FL systems when used in conjunction with hybrid ways that incorporate QKD [36][38][197].

7.1.9. Enforcing access control in edge intelligence

FL is used by edge devices in smart grids, like EV chargers and smart meters, to cooperatively train models without centrally exchanging sensitive data. Security threats to this decentralized system include illegal access to model parameters and learning procedures. By using quantum-resistant access restrictions, such as attribute-based and role-based encryption, PQC combats these risks and makes sure that only authorized devices take part. Additionally, it uses digital signatures (like Dilithium and FALCON) to secure and authenticate model updates. Secure key storage and unchangeable access records are ensured when these cryptographic technologies are integrated with hardware modules and blockchain. When combined, these safeguards preserve privacy and accountability in smart grids while defending FL against quantum and classical threats [192].

7.1.10. Supporting regulatory compliance and future-proofing

By guaranteeing adherence to laws like the EU Cybersecurity Act, NERC CIP, and GDPR and guarding against quantum risks, PQC improves FL in smart grids. Decentralized model updates and communications are protected against present and potential threats, such as "harvest-now, decrypt-later" concerns, with

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

algorithms like Dilithium, FALCON, and SPHINCS+. By incorporating these quantum-resistant methods, smart grids can maintain their alignment with changing NIST standards, encouraging crypto-agility and lowering the need for expensive system upgrades. PQC also supports blockchain and secure protocols to create immutable audit trails, which are vital for regulatory reporting and incident response. Research demonstrates that these algorithms efficiently deploy in FL while maintaining performance with minimal impact. By adopting PQC proactively, smart grid stakeholders ensure trust, resilience, and operational continuity in a quantum-threat landscape [192].

8. POST-QUANTUM SECURE BLOCKCHAIN-BASED FEDERATED LEARNING FRAMEWORK FOR SMART GRID SECURITY

8.1. Framework Components

Below are the detailed descriptions of the framework components.

8.1.1. Edge devices (Data owners)

Edge devices, such as smart meters, intelligent sensors, and DERs like solar panels, wind turbines, and battery storage systems, function as distributed nodes within the smart grid. They continuously monitor energy consumption, voltage, current, temperature, and load conditions in real time while generating and processing local data. Each device locally trains a machine learning model on its private data and transmits only the model updates, rather than raw data, to preserve privacy and reduce communication overhead.

8.1.2. Aggregator (Federated server)

The aggregator, or federated server, centrally manages the FL process by collecting model updates from all edge devices, securely aggregating them using techniques such as homomorphic encryption or secure multi-party computation, and then broadcasting the updated global model back to the devices for the next training round. Although it coordinates each phase of the learning cycle, it never accesses sensitive or raw data, thereby maintaining data privacy throughout the process.

8.1.3. Blockchain network

The blockchain network adds a decentralized and immutable layer of trust to the framework by recording hashes of model updates, aggregation results, and participant actions. It uses smart contracts to automate validation, enforce access control, maintain audit logs, and manage incentive distribution. By implementing lightweight consensus algorithms, such as PBFT or quantum-resistant PoS, scalability and energy efficiency are enhanced. This approach guarantees transparent, tamper-evident traceability across all FL activities and eliminates single points of failure.

8.1.4. Post-quantum cryptography layer

The PQC layer integrates digital signatures, key exchange protocols, and quantum-resistant encryption to safeguard computation and communication from adversaries with quantum capabilities. It employs post-quantum digital signatures to authenticate devices and confirm the integrity of sent models, and it secures model update transmissions using lattice-based or code-based encryption techniques. Additionally, the PQC layer creates safe routes of communication between edge devices and blockchain nodes or aggregators. Through these processes, it future-proofs the system against emergent quantum attacks.

8.1.5. Smart contracts

Smart contracts are self-governing scripts that run pre-programmed logic on the blockchain to increase automation and transparency while lowering the need for human intervention. They use post-quantum signatures to authenticate edge devices, reward nodes that provide legitimate model updates, and penalize or revalidate nodes that provide tainted or malicious data. To guarantee system-wide accountability and trust, these contracts also keep auditable logs that document the beginning, development, and integrity of global models.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

8.1.6. Secure communication layer

By using post-quantum TLS to provide session confidentiality and participant authentication, the secure communication layer protects all interactions between edge devices, the aggregator, and blockchain nodes. It uses end-to-end encryption to prevent tampering or interception of control messages and model updates. It also uses digital signatures and cryptographic hashes to identify any unwanted data changes.

8.1.7. Privacy-preserving mechanisms

The framework uses several mechanisms to improve individual privacy beyond FL: it employs anomaly detection engines to detect adversarial contributions or model drift, applies differential privacy by adding calibrated noise to local updates, and enforces access control policies through smart contracts that limit access to training results and model updates.

8.2. Workflow Overview

The PQS-BFL framework for smart grids combines immutable auditability, quantum-resistant security, and decentralized learning. First, FL is deployed across edge devices, including DERs, smart meters, and intelligent sensors. These devices guarantee that raw data stays on-site by locally training machine learning models using private energy consumption data. Each device computes local model updates and sends only the parameters to a coordinating node, rather than sending data to a central server. The system makes use of PQC methods, such as hash-based signatures and lattice-based encryption, to protect these connections. These techniques preserve secrecy and integrity while transmitting model changes, guarding against both conventional and quantum risks. Each device uses a post-quantum digital signature mechanism to sign its local model before sharing updates. This enables the validator or aggregator to verify the source of each update without disclosing private information. Trust and traceability are strengthened by a blockchain layer. Every model change or aggregation result is recorded by the system on a distributed ledger that is impenetrable. Blockchain-based smart contracts automate crucial processes, including consensus enforcement, incentive distribution, and participant identification. To sustain performance in the energy-constrained smart grid context, the network usually uses a scalable, energy-efficient consensus method, like PBFT or a quantum-resistant PoS. Following local changes, the aggregator uses secure aggregation methods such as secure multi-party computing or homomorphic encryption. These methods guarantee the privacy of individual updates during the aggregate procedure. Following an update to the global model, the aggregator anchors a cryptographic hash of the new model state on the blockchain and verifies the outcome. By creating a transparent and impenetrable audit trail, this procedure promotes accountability and makes it possible to validate previous training records. Mechanisms for identifying anomalies, such as poisoning attacks and malicious updates, are also included in the framework. Based on predetermined thresholds, smart contracts can flag suspicious activity, penalize misbehaving nodes, or automatically initiate re-validation procedures. To further enhance privacy, the system may employ differential privacy or inject noise, balancing privacy preservation with model accuracy. Throughout the training lifecycle, the PQS-BFL framework ensures end-to-end security, privacy, and resilience. It integrates the decentralized intelligence of FL, the cryptographic strength of post-quantum security, and the trustless coordination of blockchain technology. This integration enables secure real-time decision-making, optimizes energy management, and safeguards smart grid infrastructure against future quantum-era threats. Fig. 10 illustrates the key components and processes within the PQS-BFL framework for smart grids.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

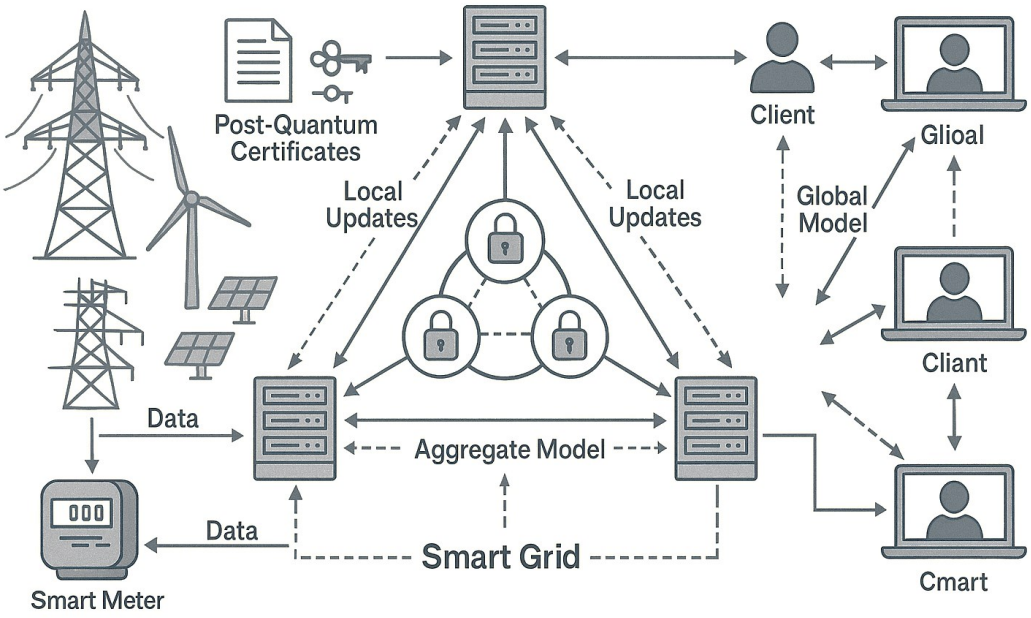

Fig. 10. Illustrates the process involved in the PQS-BFL framework for smart grids.

8.3. Roles of a PQS-BFL in Enhancing Smart Grid Security

Below are the detailed descriptions of the roles of PQS-BFL in enhancing smart grid security:

8.3.1. Secure decentralized learning for smart grid systems

Secure, decentralized learning enhances smart grid security by distributing the learning process across multiple nodes, thereby avoiding centralized vulnerabilities. It protects sensitive data from single points of failure and targets cyberattacks. A BFL framework, reinforced with PQC, adds resilience against quantum-era threats. Blockchain records each training update from substations, sensors, control centers, and microgrids on a tamper-proof ledger. FL enables these entities to train AI models locally without exposing raw data, thereby preserving privacy and reducing communication costs. This integrated approach prevents data breaches, ensures transparency, and builds trust in smart grid operations.

8.3.2. Post-quantum cryptography protection

A PQS-BFL framework protects smart grid communications from quantum-enabled threats. It utilizes quantum-resistant cryptographic algorithms, including lattice-based, hash-based, and code-based schemes, to replace the vulnerable RSA and ECC methods. Using post-quantum primitives, the blockchain layer protects transactions, verifies users, and maintains data integrity. By facilitating decentralized model training without disclosing raw data, FL improves privacy. When combined, these elements lower the possibility of breaches and protect the privacy of data. A strong, open, and future-proof foundation for safe energy management is created by this integrated approach.

8.3.3. Trust management and participant authentication

In PQS-BFL, participant identification and trust management are essential to the security of smart grids. The architecture tracks participant behavior using the immutable ledger of blockchain technology, encouraging openness and discouraging harmful action. Robust authentication prevents Sybil attacks and impersonation by confirming identities. PQC defends these procedures against dangers made possible by quantum technology. Smart contracts monitor reputation, verify updates, and automate access control. Together, these systems improve accountability, guarantee data integrity, and facilitate safe, cooperative learning in hostile settings.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

8.3.4. Data privacy preservation

By allowing decentralized model training on local devices and retaining raw data on-site, a PQS-BFL system improves data privacy in smart grids. It combats the dangers of the quantum age by including quantum-resistant encryption in FL and blockchain operations. The blockchain maintains participant anonymity while guaranteeing transparent and impenetrable logging of model updates and transactions. Cryptographic proofs and consensus procedures improve traceability and accountability. Additionally, the approach protects against model inversion and membership inference attacks by obscuring important gradients via differential privacy and post-quantum encryption. A safe, private ecosystem for cooperative grid management is produced by this combination.

8.3.5. Incentivization and reward mechanism

By providing incentives for energy providers, users, and edge devices to contribute high-quality data and computation, a PQS-BFL framework improves the security of smart grids. Smart contracts are used to impose equitable rewards based on timely updates, model improvement, and high-quality data, while a transparent, unchangeable ledger is used to track contributions. This automated, trustless method lowers the risk of fraud and does away with the necessity for central authorities. PQC protects identities and transactions from quantum assaults. While on-chain reputation discourages criminal activity, blockchain tokenization promotes honest participation. When combined, these characteristics increase security through privacy-preserving, quantum-resistant learning, encourage collaboration, and increase engagement.

8.3.6. Tamper-resistant auditability and logging

By permanently recording all transactions and data exchanges within a PQS-BFL architecture, tamper-resistant auditability and logging improve smart grid security. To stop unwanted changes, the system records model updates, data contributions, and system events. The verifiability and transparency of blockchain technology provide precise, unchangeable records. These records are shielded against potential quantum attacks by PQC. Real-time compliance enforcement, anomaly detection, and action tracing are all possible for grid operators. In addition to supporting forensic investigation and ensuring non-repudiation, this audit trail fortifies defenses against sophisticated cyberattacks.

8.3.7. Resilience against model poisoning and byzantine attacks

Smart grid resilience against Byzantine attacks and model poisoning is enhanced by a PQS-BFL framework. It employs blockchain technology to transparently record every node's contribution, facilitating the quick identification and isolation of bad actors. FL protects privacy by enabling nodes to work together to train models without exchanging raw data. Unreliable or tainted updates are filtered out before they have an impact on the global model by robust consensus and anomaly detection. In the age of quantum computing, PQC safeguards against attacks and secures communications. The framework guarantees reliable decision-making in hostile contexts by fusing secure aggregation, anomaly detection, and authenticated updates.

8.3.8. Scalability and interoperability across grid entities

A PQS-BFL system guarantees scalability and interoperability, which enhances smart grid security. To handle growing data quantities and linked devices, it makes use of scalable algorithms and cutting-edge blockchain strategies like sharding, sidechains, or DAGs. Real-time processing and smooth connectivity between cloud servers, control units, and IoT devices are made possible by the framework. To synchronize learning across many platforms and standards, it offers interoperable protocols. Data integrity and privacy are safeguarded by incorporating lightweight PQC techniques. This cohesive strategy ensures safe and effective grid operations while defending against both classical and quantum cyberthreats.

Through the assurance of confidentiality, integrity, availability, and resilience, a PQS-BFL framework improves the security of smart grids. It offers a future-ready solution that safeguards intelligent power infrastructure by fusing quantum-resistant cryptography, decentralized trust mechanisms, and privacy-preserving AI.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

8.4. Benefits of PQS-BFL in Smart Grid Security

The following are some advantages of using PQS-BFL to improve smart grid security:

8.4.1. Quantum-resistant security

The threat that quantum computing presents to smart grids is mitigated by quantum-resistant security, which substitutes PQC techniques for weak algorithms like RSA and ECC. These techniques, which include multivariate polynomial schemes, lattice-based, and hash-based approaches, rely on mathematical issues that are inefficient for quantum computers to handle. By incorporating these strategies into FL and blockchain, sensitive smart grid data is shielded from tampering and exposure. During distributed training and consensus, the system protects communications, digital signatures, encryption, and key creation. As a result, BFL defends against adversaries with quantum capabilities while maintaining dependable, privacy-preserving smart grid operations. Critical infrastructure is future-proofed with this strategy for sustained resilience in the post-quantum age.

8.4.2. Decentralized trust

By dispersing transaction recording and verification among separate nodes, blockchain integration with FL improves smart grid security by removing single points of failure. Without depending on a central authority, these nodes swiftly identify and reject malicious inputs by cooperatively authenticating and aggregating model updates. This architecture is protected from new quantum risks by PQC algorithms. The solution ensures accountability and transparency for authorized parties by recording each transaction on an immutable blockchain ledger. This audit trail aids authorities in confirming adherence to security regulations and discourages harmful activity. Together, BFL creates a foundation that is impenetrable and protects privacy, allowing the smart grid to function safely and effectively.

8.4.3. Privacy preservation

By doing away with the requirement for centralized data collecting and storage, PQS-BFL improves smart grid privacy. To reduce data exposure, smart grid nodes train models locally and only exchange encrypted updates. PQC protects all model exchanges and communications from quantum threats. Blockchain guarantees transparent transaction records and tamper-proof, decentralized access control. Only authorized entities are permitted to access and update smart contracts due to their stringent participation criteria. Together, these steps provide a strong privacy foundation for smart grid protection.

8.4.4. Secure model aggregation

By decentralizing and safeguarding the model aggregation process, BFL ensures smart grid collaboration. To provide immutability and transparency, each node publishes its locally trained changes as blockchain transactions. Data poisoning and model drift are avoided by the decentralized consensus system, which verifies updates by thwarting harmful or incorrect contributions. PQC protects against upcoming quantum dangers. When combined, these technologies give smart grids a secure, impenetrable, and private learning environment.

8.4.5. Robust against adversarial attacks

To jeopardize the integrity of the system, adversaries in smart grids may alter data, interfere with communications, or undermine machine learning models. PQS-BFL uses cutting-edge protections to fend off these threats. By securing communications with PQC, it guards against quantum-enabled attacks on local model changes. Blockchain makes ensuring that updates are recorded without tampering, which makes auditability and real-time verification possible. FL lessens vulnerability to centralized assaults by storing raw data locally. Integrated anomaly detectors highlight questionable activities, enhancing the smart grid's dependability and credibility.

8.4.6. Transparent auditability

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

By creating an unchangeable and traceable record of every learning activity, transparent auditability in BFL improves smart grid security. To guard against manipulation or deletion, the blockchain records every model update, aggregate, and inter-node communication. Operators and auditors can check the integrity of data in real time or after the fact thanks to this decentralized structure. It makes it possible to identify abnormalities, unauthorized modifications, or malicious activity early on. The approach guarantees responsibility and discourages insider threats by assigning a specific participant to each update. The audit trail is further shielded from both classical and quantum attacks by PQC.

8.4.7. Efficient key management

Strong key management between dispersed devices is essential for secure communication in smart grids. PQC-enhanced BFL protects encryption keys from quantum attacks. Without requiring a central authority, it distributes, stores, and revokes keys via decentralized, immutable ledgers. By automating key creation, renewal, and revocation, smart contracts guarantee uniform application of rules and guidelines. This integration improves security and streamlines operations for devices that are spread out geographically. In the quantum era, smart grids therefore accomplish scalable, reliable, and trustworthy data sharing.

8.4.8. Enhanced data integrity

Accurate decision-making in smart grids depends on preserving data integrity across dispersed devices. PQS-BFL enhances this integrity by fusing decentralized, privacy-preserving training with the tamper-proof ledger of blockchain technology. Unauthorized changes are prevented by recording every model update and data exchange as an immutable transaction. These records are protected from potential quantum threats by PQC. The system guards against replay and poisoning attempts on both raw data and aggregated model parameters. In the face of changing cyberthreats, our strategy guarantees that smart grids stay accurate, reliable, and safe.

8.4.9. Improved scalability

The scalability of smart grid security is increased by integrating FL with a post-quantum secure blockchain. IoT devices, smart meters, and DERs all contribute to the vast amounts of data generated by smart grids. By processing this data locally, FL lessens network congestion and server strain. Model updates are safely coordinated by blockchain without the need for a centralized authority. As the network expands, its consensus process effectively aggregates updates. PQC ensures safe and scalable smart grid operations by defending the system against quantum attacks.

8.4.10. Regulatory compliance

Smart grids may now adhere to energy-specific requirements and strict data protection rules like the CCPA and GDPR thanks to PQS-BFL. Maintaining the decentralization of raw customer data, it facilitates data minimization and lowers vulnerability. The method reduces the risk of a breach by training models cooperatively without transmitting private information to central servers. Blockchain guarantees access for regulatory audits and an unchangeable, transparent record of developments. These records are shielded against potential quantum attacks by PQC. By protecting sensitive data during smart grid operations, this method lowers compliance risks and fosters confidence.

9. REAL-WORLD IMPLEMENTATIONS AND CASE STUDIES

Researchers have developed several prototypes and conducted pilot deployments that demonstrate the viability of PQS-BFL systems in real-world smart grid environments. These implementations highlight practical use cases and confirm the feasibility of integrating such advanced technologies into operational energy infrastructures. Real-world implementations and use cases include:

9.1. PQS-BFL for Distributed Intrusion Detection in Smart Substations (Germany, Fraunhofer ISE Pilot)

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

The Fraunhofer Institute for Solar Energy Systems (ISE) in Germany piloted the PQS-BFL framework to enhance distributed intrusion detection in smart substations, addressing critical security and data privacy challenges in modern energy infrastructure. Traditional centralized systems often fall short due to latency, scalability, and privacy limitations; PQS-BFL overcomes these by enabling substations to collaboratively train a shared intrusion detection model without exposing raw network data. Each substation operates a local model and shares only encrypted updates through the FL process. To ensure data integrity and transparency, the system uses a customized Hyperledger Fabric blockchain with NIST-approved post-quantum signatures. A lattice-based PQC protocol, such as CRYSTALS-Kyber, secures communications and parameter exchanges. The framework integrates differential privacy and secure aggregation to protect sensitive information. It employs a quality control module that filters out low-quality or malicious updates, strengthening the model's robustness and trustworthiness. During the pilot, intelligent electronic devices effectively learned to detect grid anomalies, identifying threats like FDI and DoS attacks with up to 92% accuracy. The decentralized, blockchain-supported approach eliminated single points of failure, ensured tamper-proof audit trails, and demonstrated strong resilience against quantum-era adversaries, validating PQS-BFL's scalability, security, and privacy-preserving capabilities in real-world substation environments.

9.2. EV Charging Infrastructure Management in South Korea (KAIST and KEPCO Joint Testbed)

South Korea's national utility company, KEPCO, in collaboration with the Korea Advanced Institute of Science and Technology (KAIST), has developed and tested a PQS-BFL model to enhance secure FL at EV charging stations. To address challenges in data privacy, system latency, and scalability for real-time power demand forecasting, the researchers utilized FrodoKEM-based post-quantum encryption to safeguard FL updates from edge nodes, including individual charging points. They recorded these updates and access requests on a permission blockchain, using post-quantum digital signatures to authenticate contributors and maintain training integrity. Smart contracts enforced policies on update frequency and dropout tolerance, mitigating poisoning attack risks. The PQS-BFL model successfully preserves data privacy without sacrificing forecasting accuracy, significantly reduces latency compared to traditional cloud-based aggregation, and scales efficiently to support over 300 edge devices with minimal model divergence, demonstrating its robustness in large-scale deployments.

9.3. Renewable Energy Microgrid Coordination in Canada (University of Waterloo – Smart Grid Laboratory)

A prototype of the PQS-BFL system was deployed in a microgrid environment consisting of solar photovoltaic (PV) arrays, energy storage units, and smart inverters. Each microgrid controller independently trained a demand-response model using privacy-preserving FL, keeping local data on-site to protect privacy while collaboratively improving the model. To ensure the integrity and verifiability of model updates and coordination records, the researchers integrated a hybrid blockchain layer secured with post-quantum digital signatures, such as Dilithium, which prevented tampering and ensured transparent coordination among distributed controllers. They also applied secure aggregation protocols to mask individual model contributions, thereby effectively reducing the risks associated with model inversion and inference attacks. The implementation enabled secure, decentralized coordination of energy assets without revealing sensitive demand profiles, demonstrated resilience against quantum-capable adversaries, and improved demand prediction accuracy, resulting in up to a 12% increase in load balancing efficiency across the microgrid.

10. OPEN ISSUES AND CHALLENGES

Implementing a PQS-BFL system in smart grid security presents several open issues and challenges, as described below.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

10.1. Quantum-resistant cryptography integration

Integrating PQC into BFL for smart grid security introduces significant design and performance challenges. PQC algorithms, such as CRYSTALS-Kyber and Dilithium, require larger keys and ciphertexts, which increase latency and resource usage in constrained devices. These demands hinder real-time operations and strain both blockchain (e.g., consensus, signatures) and FL mechanisms (e.g., secure aggregation). Replacing ECDSA with post-quantum signatures enlarges block sizes and slows synchronization. Smart contracts and secure aggregation protocols must execute quantum-safe operations within tight computational budgets. The absence of formal quantum-resilient security models highlights the urgent need for scalable, efficient, and trustworthy post-quantum BFL frameworks [5][39][40].

10.2. Computational and communication overhead

Implementing PQS-BFL in smart grids is challenging due to the high computational and communication overhead of quantum-resistant cryptography. These algorithms require significantly larger keys, signatures, and ciphertexts than traditional schemes, thereby increasing memory and bandwidth usage. For instance, while ECDSA signatures are 64 bytes, CRYSTALS-Dilithium and Kyber generate much larger cryptographic artifacts. Resource-limited edge devices, such as smart meters and RTUs, struggle with heavy computations, resulting in slower processing and increased energy consumption. The overhead delays model training, inflates blockchain transactions, and reduces system throughput. It also burdens communication channels, threatening time-sensitive smart grid operations [198].

10.3. Scalability of blockchain for FL

As smart grids integrate more devices, ensuring scalable BFL with post-quantum security becomes crucial. The blockchain must handle increasing transactions, model updates, and authentications quickly despite the overhead of larger post-quantum keys and signatures. These larger cryptographic elements increase block sizes, slow down propagation, reduce throughput, and strain resource-limited edge validators. Frequent encrypted model updates in FL intensify this load. Solutions such as sharding, off-chain storage, and layer-2 techniques can help. However, they also introduce architectural and security challenges, particularly in maintaining quantum-safe integrity through cryptographic commitments and zero-knowledge proofs. Without effective scalability, these systems risk delayed consensus, poor real-time performance, and failure in large-scale deployments [198][199].

10.4. Data privacy and model leakage

FL protects data privacy by sharing model parameters instead of raw data, but these parameters remain vulnerable to inference attacks by post-quantum adversaries. PQC methods, like lattice-based encryption, secure confidentiality and integrity but do not entirely prevent privacy leaks from model updates. Quantum-enabled attackers can infer sensitive information from shared gradients or parameters in smart grids. Integrating privacy-preserving techniques, such as homomorphic encryption, differential privacy, or secure multi-party computation, reduces this risk but introduces significant computational and communication overhead, making deployment in resource-limited smart grids challenging. Although blockchain improves auditability and trust by recording updates and smart contracts, it can leak metadata that attackers exploit. Securing BFL in the quantum era requires combining quantum-resistant cryptography with efficient privacy methods and metadata-protective blockchain protocols tailored to the constraints of the smart grid [71][200].

10.5. Consensus mechanism vulnerabilities

Post-quantum environments expose traditional blockchain consensus mechanisms, such as PoW, PoS, and PBFT, to vulnerabilities, as quantum algorithms like Shor's can break classical signatures, including ECDSA. Attackers with quantum capabilities could forge signatures and manipulate consensus messages, thereby threatening the integrity of blockchain systems. Although post-quantum signatures, such as Dilithium and Falcon, resist these attacks, their larger size and complex verification process slow transaction propagation, especially in bandwidth- and latency-sensitive smart grids. Resource-limited devices struggle with the computational demands, which can lead to centralization and undermine decentralization.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Transitioning protocols face challenges in coordination and backward compatibility, while hybrid schemes increase overhead and complexity. Quantum adversaries could exploit these weaknesses to launch forks or double-spending attacks, thereby endangering the security of BFL in smart grids [201].

10.6. Robustness against adversarial attacks

Adversaries are increasingly targeting smart grids and FL systems with attacks such as model poisoning, Byzantine failures, and Sybil attacks. Defending these threats using post-quantum secure authentication in BFL remains complex and underexplored. Although PQC protects cryptographic primitives, attackers can still compromise model training, data integrity, communication, or consensus. Attackers inject malicious updates to degrade models or exploit smart contract flaws despite quantum-safe signatures preventing forgery. Moreover, the high resource demands of post-quantum methods may introduce new vulnerabilities. The evolving threat landscape demands forward-secure protocols to protect against both classical and future quantum adversaries [202][203].

10.7. Interoperability among heterogeneous devices

Implementing PQS-BFL in smart grids poses challenges to interoperability due to the diversity of devices and systems. Resource-constrained edge devices, such as smart meters and sensors, struggle with the larger key sizes and complex operations of PQC, resulting in performance bottlenecks and delayed model updates. Legacy devices often require firmware redesigns and protocol changes to support these algorithms. During the transition, systems must maintain backward compatibility between classical and quantum-resistant technologies. Varying network protocols and limited bandwidth complicate secure data transmission, as larger packets can cause fragmentation and latency. These issues threaten the efficiency and responsiveness of smart grid operations [36][204][208].

10.8. Energy efficiency

Implementing PQS-BFL in smart grids strains the energy budgets of edge devices, such as smart meters and sensors. PQC increases computational complexity and key sizes, demanding more processing power and longer computation times for encryption, key generation, and verification. These heavier operations drain device batteries more quickly and increase maintenance costs. Larger keys and signatures also increase bandwidth usage, thereby elevating energy consumption during data transmission, particularly in wireless settings. Blockchain tasks, such as consensus and transaction validation, become more energy-intensive with the introduction of post-quantum protocols, thereby extending processing times. This challenge intensifies in permissionless and consortium blockchains that require frequent consensus interactions [198][205][209][210].

10.9. Regulatory and standardization challenges

Regulatory and standardization challenges hinder the adoption of PQS-BFL in smart grid security. Regulatory bodies have yet to provide clear guidelines, causing uncertainty among developers and operators. The evolving cryptographic standards and lack of universal acceptance complicate interoperability and long-term planning. Stakeholders risk fragmentation and weakened security without standardized frameworks that align with existing certifications and privacy laws. Coordinating experts, operators, and policymakers is crucial to developing practical and enforceable standards for gradual migration. Addressing global regulatory inconsistencies requires proactive and collaborative efforts to enable secure and compliant deployment [198][206][207].

10.10. Long-term security and upgradability

To ensure long-term security against quantum threats, BFL systems for smart grids must adopt cryptographic agility, allowing seamless upgrades of cryptographic primitives and consensus protocols without operational disruption. As quantum computing progresses, flexible architectures should support hybrid frameworks that securely combine legacy and post-quantum algorithms during transitions. These

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

systems must manage compatibility across diverse, resource-limited nodes while implementing robust key management for scalable key renewal, revocation, and distribution. They must also maintain high reliability and availability by utilizing upgrade protocols that minimize downtime, preserve node trust, and safeguard the integrity of both the FL process and the blockchain ledger [198].

11. FUTURE RESEARCH DIRECTIONS

Below are the detailed descriptions of the future research directions for the successful implementation of PQS-BFL for smart grid security:

- Design of lightweight PQC algorithms for resource-constrained devices: PQC provides quantum-resistant security, but its algorithms typically require substantial computational resources. Since smart grid edge devices, such as smart meters and IoT sensors, operate with constrained processing power and energy, researchers should focus on developing lightweight PQC schemes. In particular, compact lattice-based or code-based cryptosystems can deliver robust security while reducing the strain on limited device resources.
- Scalable and efficient blockchain architectures: Traditional blockchain architectures face significant challenges in terms of scalability and latency, particularly in high-frequency data environments such as smart grids. To address these limitations, future efforts aim to develop quantum-resistant consensus mechanisms, such as lattice-based PoW, as well as sharded, DAG-based, and layer-2 blockchain protocols specifically designed to support post-quantum security and the high data throughput demands of FL.
- Privacy-preserving FL with post-quantum techniques: FL remains vulnerable to threats like model inversion and gradient leakage. To address these issues, future research can enhance FL protocols by integrating post-quantum secure multi-party computation, homomorphic encryption, or zero-knowledge proofs. These techniques can ensure verifiable and confidential model updates while preserving training efficiency.
- Quantum-resilient threat modeling in smart grid environments: Quantum adversaries pose novel threat models, including quantum eavesdropping and Grover-based key search. Future research should develop quantum-resilient threat models that account for hybrid classical-quantum attack vectors, federated poisoning attacks in the presence of quantum adversaries, and quantum-enabled MitM attacks targeting FL communications and blockchain infrastructures.
- Incentive mechanisms for FL participation in post-quantum settings: Blockchain supports decentralized incentives for participation in FL, yet the development of post-quantum secure tokenization and reputation systems remains largely unexplored. Future research should focus on designing quantum-secure smart contracts for token distribution, implementing trust scoring mechanisms based on lattice-based signatures, and developing game-theoretic models that resist quantum-based manipulation.
- Cross-domain post-quantum BFL interoperability standards: The smart grid ecosystem integrates generation, distribution, and consumption domains, often involving diverse systems. To achieve seamless integration, developers must create interoperable, post-quantum secure APIs, protocols, and standards that enable FL and blockchain across various utilities and vendors.
- Dynamic aggregation and model personalization under post-quantum constraints: In real-world smart grid scenarios, data distributions are non-IID, and device availability varies. Future research should develop dynamic federated aggregation techniques that tolerate dropout, design personalized FL models that balance global learning with local adaptation and create post-quantum-secure schemes for selective aggregation and model pruning.
- Energy-efficient consensus and FL under post-quantum security: PQC and blockchain technologies significantly increase energy demands. Researchers should develop green post-quantum consensus protocols, such as proof-of-space-time and PQ-DPoS, design energy-aware federated scheduling algorithms, and optimize communication alongside cryptographic workloads to enhance sustainability.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

- Post-quantum secure model auditing and explainability: Ensuring secure and transparent behavior in FL models is crucial for maintaining trust. Researchers are exploring quantum-secure logging of model decisions on blockchain, developing auditable model behavior verification using post-quantum zero-knowledge proofs, and advancing Explainable AI techniques that operate effectively under post-quantum encryption constraints.
- Resilient deployment strategies in quantum-enabled smart grid ecosystems: Deploying post-quantum BFL in live smart grids challenges fault tolerance, synchronization, and governance. Future efforts should focus on developing digital twin simulations of quantum-safe FL-blockchain systems, creating adaptive deployment frameworks that leverage edge-cloud orchestration, and designing policy-driven governance models to ensure grid security and stakeholder accountability against quantum threats.

12. CONCLUSIONS

The rapid integration of advanced digital technologies into smart grids has significantly improved operational efficiency, control, and sustainability.

References

[1] S. Yilmaz, and M. Dener, "Security with Wireless Sensor Networks in Smart Grids: A Review," *Symmetry*, vol. 16, no. 10, pp. 1–40, 2024. https://doi.org/10.3390/sym16101295

[2] A. M. Etman, M. S. Abdalzaher, A. Emran, A. Yahya, and M. Shaaban, "A survey on machine learning techniques in smart grids based on wireless sensor networks," *IEEE Access*, vol. 13, pp. 2604-2627, 2024. https://doi.org/10.1109/access.2024.3524097

[3] K. Ramana, and H. Sahu, "Performance Analysis of RIS-Assisted Smart Grid Wide Area Network With RF Energy Harvesting," *IEEE Access*, vol. 13, pp. 23959-23970, 2025. https://doi.org/10.1109/ACCESS.2025.3536890

[4] N. Xiao, Z. Wang, and X. Sun, "A secure and efficient authentication scheme for vehicle to grid in smart grid," *Frontiers in Physics*, vol. 13, pp. 1–11, 2025. https://doi.org/10.3389/fphy.2025.1529638

[5] J. Xiong, L. Shen, Y. Liu, and X. Fang, "Enhancing IoT security in smart grids with quantum-resistant hybrid encryption," *Scientific Reports*, vol. 15, no. 1, pp. 1–12, 2025. https://doi.org/10.1038/s41598-024-84427-8

[6] C. Tharani, C. Ashritha, and P. V. Manitha, "Data Security in Smart Grid Using Cryptographic Algorithms," 2025 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE), Shivamogga, India, 24-25 April 2025, pp. 1-5, doi: 10.1109/AMATHE65477.2025.11080901.

[7] S. Selvarajan, H. Manoharan, T. Al-Shehari, H. Alsalman, and T. Alfakih, "Smart Grid Security Framework for Data Transmissions with Adaptive Practices Using Machine Learning Algorithm," *Computers, Materials & Continua*, vol. 82, no. 3, pp. 4339–4369, 2025. https://doi.org/10.32604/cmc.2025.056100

[8] J. P. A. Yaacoub, H. N. Noura, O. Salman, and K. Chahine, "Toward secure smart grid systems: risks, threats, challenges, and future directions," *Future Internet*, vol. 17, no. 7, pp. 1–87, 2025. https://doi.org/10.3390/fi17070318

[9] J. Zhu, G. Wang, Q. Chen, Y. Huang, and W. Yang, "Application prospect of integration of smart grid and Internet of Things technology in distribution automation," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 127b, pp. 7531-7547, 2025. https://doi.org/10.61091/jcmcc127b-411

[10] N. Shrivastava, "Optimizing Smart Grids for Distributed Energy Resource Integration and Management," *Journal of Information Systems Engineering and Management*, vol. 10, no. 5s, pp. 421-427, 2025. https://doi.org/10.52783/jisem.v10i5s.647

[11] P. Biswas, A. Rashid, A. Habib, M. Mahmud, S. Motakabber, S. Hossain, M. Rokonuzzaman, A. Molla, Z. Harun, M. Khan, W. Cheng, and T. Lei, "Vehicle to Grid: Technology, Charging Station, Power Transmission, Communication Standards, Techno-Economic Analysis, Challenges, and Recommendations," *World Electric Vehicle Journal,* vol. 16, no. 3, pp. 1-35, 2025. https://doi.org/10.3390/wevj16030142

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[12] T. Krishnan, P. Satpathy, V. Ramachandaramurthy, Z. Dollah, S. Pulenthirarasa, and A. Ramasamy, "Optimizing Vehicle-to-Grid Systems: Smart Integration of Shared Autonomous and Conventional Electric Vehicles," *eTransportation*, vol. 24, pp. 100401, 2025. https://doi.org/10.1016/j.etran.2025.100401

[13] C. Ogbogu, J. Thornburg, and S. Okozi, "Smart Grid Fault Mitigation and Cybersecurity with Wide-Area Measurement Systems: A Review," *Energies*, vol. 18, no. 4, pp. 1-26, 2025. https://doi.org/10.3390/en18040994

[14] V. Ethirajan, and S. P. Mangaiyarkarasi, "An in-depth survey of latest progress in smart grids: paving the way for a sustainable future through renewable energy resources," *Journal of Electrical Systems and Information Technology*, vol. 12, no. 1, pp. 1–46, 2025. https://doi.org/10.1186/s43067-025-00195-z

[15] L. Gabriel, J. Adebisi, N. Leokadia, and D. Chembe, "Investigation of Smart Grid Technologies Deployment for Energy Reliability Enhancement in Electricity Distribution Networks," *Franklin Open*, vol. 10, pp. 1-17, 2025. https://doi.org/10.1016/j.fraope.2025.100227

[16] S. Lalit, "Smart Grid Architecture: An Overview," 2025 IEEE International Conference on Power Systems and Smart Grid Technologies (PSSGT), Chongqing, China, 11-13 April 2025, pp. 225-229, doi: 10.1109/PSSGT64932.2025.11033792.

[17] N. Jain, B. Pillai and N. Singh, "Green IoT-Based Smart Grid: Implementing Intelligent Demand-Response Systems for Energy Sustainability," 2025 2nd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India, 07-08 May 2025, pp. 1-6, doi: 10.1109/RMKMATE64874.2025.11042574.

[18] Y. Yang, M. Liu, Q. Zhou, H. Zhou and R. Wang, "A Blockchain Based Data Monitoring and Sharing Approach for Smart Grids," IEEE Access, vol. 13, pp. 122496-122505, 2025, doi: 10.1109/ACCESS.2019.2952687.

[19] N. P. L. Dushing, N. P. G. Wakhure, N. S. Kazi, N. S. S. Ramteke, N. A. B. Kasar, N. S. Wasu, and N. S. S. Waghmode, "Analysis of smart grid technologies in the electrical power industry," *Nanotechnology Perceptions*, pp. 1351–1358, 2024. https://doi.org/10.62441/nano-ntp.vi.3905

[20] S. Qazi, B. A. Khawaja, A. Alamri, and A. AlKassem, "Fair energy trading in Blockchain-Inspired smart grid: Technological barriers and future trends in the age of electric vehicles," *World Electric Vehicle Journal*, vol. 15, no. 11, pp. 1–28, 2024. https://doi.org/10.3390/wevj15110487

[21] S. Amanlou, M. K. Hasan, U. A. Mokhtar, K. M. Malik, S. Islam, S. Khan, M. A. Khan, and M. A. Khan, "Cybersecurity Challenges in Smart Grid Systems: Current and Emerging Attacks, Opportunities, and Recommendations," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 1965–1997, 2025. https://doi.org/10.1109/ojcoms.2025.3545153

[22] M. A. Alomari, M. N. Al-Andoli, M. Ghaleb, R. Thabit, G. Alkawsi, J. A. J. Alsayaydeh, and A. S. A. Gaid, "Security of Smart Grid: cybersecurity issues, potential cyberattacks, major incidents, and future directions," *Energies*, vol. 18, no. 1, pp. 1–34, 2025. https://doi.org/10.3390/en18010141

[23] N. Ibrahim, and R. Kashef, "Exploring the emerging role of large language models in smart grid cybersecurity: a survey of attacks, detection mechanisms, and mitigation strategies," *Frontiers in Energy Research*, vol. 13, pp. 1–23, 2025. https://doi.org/10.3389/fenrg.2025.1531655

[24] S. H. Mohammed, A. Al-Jumaily, M. S. J. Singh, V. P. G. Jiménez, A. S. Jaber, Y. S. Hussein, M. M. A. K., Al-Najjar, and D. Al-Jumeily, "A review on the evaluation of feature selection using machine learning for Cyber-Attack detection in smart Grid," *IEEE Access*, vol. 12, pp. 44023–44042, 2024. https://doi.org/10.1109/access.2024.3370911

[25] B. Paul, A. Sarker, S. H. Abhi, S. K. Das, M. F. Ali, M. M. Islam, M. R. Islam, S. I. Moyeen, M. F. R. Badal, M. H. Ahamed, S. K. Sarker, P. Das, M. M. Hasan, and N. Saqib, "Potential smart Grid vulnerabilities to cyber attacks: current threats and existing mitigation strategies," *Heliyon*, vol. 10, no. 19, pp. 1–26, 2024. https://doi.org/10.1016/j.heliyon.2024.e37980

[26] G. Zhang, W. Gao, Y. Li, X. Guo, P. Hu, and J. Zhu, "Detection of false data injection attacks in a smart grid based on WLS and an adaptive interpolation extended Kalman filter," *Energies*, vol. 16, no. 20, pp. 1–20, 2023. https://doi.org/10.3390/en16207203

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[27] R. Shen, H. Zhang, B. Chai, W. Wang, G. Wang, B. Yan, and J. Yu, "BAFL-SVM: A blockchain-assisted federated learning-driven SVM framework for smart agriculture," *High-Confidence Computing*, vol. 5, pp. 1–10, 2025. https://doi.org/10.1016/j.hcc.2024.100243

[28] R. Rahman, N. Kumar and D. C. Nguyen, "Electrical Load Forecasting in Smart Grid: A Personalized Federated Learning Approach," 2025 IEEE 22nd Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10-13 January 2025, pp. 1-2, doi: 10.1109/CCNC54725.2025.10976072.

[29] A. Arya, "Combining Federated Learning and Blockchain to Enhance Cloud Storage Security," European Journal of Applied Science, Engineering and Technology, vol. 3, no. 1, pp. 4-16, 2025. DOI: 10.59324/ejaset.2025.3(1).01

[30] M. Shalan, M. R. Hasan, Y. Bai, and J. Li, "Enhancing Smart Home Security: Blockchain-Enabled Federated Learning with Knowledge Distillation for Intrusion Detection," *Smart Cities*, vol. 8, no. 1, pp. 1–30, 2025. https://doi.org/10.3390/smartcities8010035

[31] J. Yu, H. Yao, K. Ouyang, X. Cao, and L. Zhang, "BPS-FL: Blockchain-Based Privacy-Preserving and Secure Federated Learning," *Big Data Mining and Analytics*, vol. 8, no. 1, pp. 189–213, 2025. https://doi.org/10.26599/bdma.2024.9020053

[32] M. Firdaus, H. T. Larasati, and K. Hyune-Rhee, "Blockchain-based federated learning with homomorphic encryption for privacy-preserving healthcare data sharing," *Internet of Things*, vol. 31, pp. 1–17, 2025. https://doi.org/10.1016/j.iot.2025.101579

[33] H. Wang, H. Gao, T. Ma, C. Li, and T. Jing, "A hierarchical blockchain-enabled distributed federated learning system with model-contribution based rewarding," *Digital Communications and Networks*, vol. 11, no. 1, pp. 35–42, 2025. https://doi.org/10.1016/j.dcan.2024.07.002

[34] W. Ning, Y. Zhu, C. Song, H. Li, L. Zhu, J. Xie, T. Chen, T. Xu, X. Xu, and J. Gao, "Blockchain-Based Federated Learning: A survey and new perspectives," *Applied Sciences*, vol. 14, no. 20, pp. 1–35, 2024. https://doi.org/10.3390/app14209459

[35] C. Cui, H. Du, Z. Jia, Y. He, and L. Wang, "Blockchain-Enabled Federated Learning with Differential Privacy for Internet of Vehicles," *Computers, Materials & Continua*, vol. 81, no. 1, pp. 1581–1593, 2024. https://doi.org/10.32604/cmc.2024.055557

[36] S. Ren, E. Kim, and C. Lee, "A scalable blockchain-enabled federated learning architecture for edge computing," *PLoS ONE*, vol. 19, no. 8, pp. 1–28, 2024. https://doi.org/10.1371/journal.pone.0308991

[37] M. M. Orabi, O. Emam, and H. Fahmy, "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review," *Journal of Big Data*, vol. 12, no. 1, pp. 1–25, 2025. https://doi.org/10.1186/s40537-025-01099-5

[38] S. Garg, Y. Gayatri, A. S. Kausthub and S. M. Rajagopal, "Enhancing Smart Grid Security with Quantum Cryptography: A BB84-based Framework," 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 05-07 February 2025, pp. 549-554, doi: 10.1109/IDCIOT64235.2025.10914688.

[39] J. Jabłoński, and R. Dylewski, "Quantum-Resistant Cryptography for Smart Metering in Smart Grid Systems," *Energies*, vol. 18, no. 5, pp. 1-13, 2025. https://doi.org/10.3390/en18051204

[40] A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero, and M. Polsinelli, "Integrating Post-Quantum cryptography and blockchain to secure Low-Cost IoT devices," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 2, pp. 1674–1683, 2024. https://doi.org/10.1109/tii.2024.3485796

[41] X. Qin, and R. Xu, "Efficient Post-Quantum Cross-Silo Federated Learning Based on Key Homomorphic Pseudo-Random Function," *Mathematics*, vol. 13, no. 9, pp. 1-24, 2025. https://doi.org/10.3390/math13091404

[42] Y. Zhang, R. Behnia, A. Yavuz, R. Ebrahimi, and E. Bertino, "Efficient Full-Stack Private Federated Deep Learning with Post-Quantum Security," *IEEE Transactions on Dependable and Secure Computing*, pp. 1-17, 2025. https://doi.org/10.1109/tdsc.2025.3568704

[43] J. Ahmad, M. Rizwan, S. F. Ali, U. Inayat, H. A. Muqeet, M. Imran, and T. Awotwe, "Cybersecurity in smart microgrids using blockchain-federated learning and quantum-safe approaches: A comprehensive review," *Applied Energy*, vol. 393, pp. 126118, 2025. https://doi.org/10.1016/j.apenergy.2025.126118

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[44] C. Ren, Z. Dong, H. Yu, M. Xu, Z. Xiong, and D. Niyato, "ESQFL: Digital Twin-Driven Explainable and Secured Quantum Federated Learning for Voltage Stability Assessment in Smart Grids," *IEEE Journal of Selected Topics in Signal Processing*, vol. 18, pp. 964-978, 2024. https://doi.org/10.1109/JSTSP.2024.3485878

[45] I. Parvez, M. Aghili, H. Riggs, A. Sundararajan, A. I. Sarwat, and A. K. Srivastava, "A novel authentication management for the data security of smart Grid," *IEEE Open Access Journal of Power and Energy*, vol. 11, pp. 218–230, 2024. https://doi.org/10.1109/oajpe.2024.3393971

[46] A. Bedi, J. Ramprabhakar, R. Anand, U. Kumaran, V. P. Meena, and I. A. Hameed, "A novel blockchain supported hybrid authentication and handshake algorithm for smart grid," *IEEE Access*, vol. 12, pp. 177589–177608, 2024. https://doi.org/10.1109/access.2024.3505535

[47] K. Reindl, C. Dalhammar, and E. Brodén, "Circular Economy Integration in smart Grids: a nexus for sustainability," *Circular Economy and Sustainability*, vol. 4, no. 3, pp. 2119–2145, 2024. https://doi.org/10.1007/s43615-024-00375-5

[48] Y. Ishaq, A. S. Prince, G. G. J. Claude, and T. M. Di Bebe, "Decentralized framework for securing smart grids using blockchain and machine learning," *International Journal for Research in Applied Science and Engineering Technology*, vol. 13, no. 1, pp. 679–685, 2025. https://doi.org/10.22214/ijraset.2025.66079

[49] J. Powell, A. McCafferty-Leroux, W. Hilal, and S. A. Gadsden, "Smart grids: A comprehensive survey of challenges, industry applications, and future trends," *Energy Reports*, vol. 11, pp. 5760–5785, 2024. https://doi.org/10.1016/j.egyr.2024.05.051

[50] U. Khare, A. Malviya, S. K. Gawre, and A. Arya, "Cyber Physical Security of a Smart Grid: A review," 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 18-19 February 2023, pp. 1–6. https://doi.org/10.1109/sceecs57921.2023.10062966

[51] A. E. Maghraoui, H. E. Hadraoui, Y. Ledmaoui, N. E. Bazi, N. Guennouni, and A. Chebak, "Revolutionizing smart grid-ready management systems: A holistic framework for optimal grid reliability," *Sustainable Energy Grids and Networks,* vol. 39, pp. 1–15, 2024. https://doi.org/10.1016/j.segan.2024.101452

[52] M. J. Abudin, S. Thokchom, R. T. Naayagi, and G. Panda, "Detecting false data injection attacks using Machine Learning-Based approaches for smart grid networks," *Applied Sciences*, vol. 14, no. 11, pp. 1–16, 2024. https://doi.org/10.3390/app14114764

[53] L. Xiao, D. Han, X. Meng, D. He, and M. Ke, "A security protection scheme for abnormal transaction data in smart grid system," *International Journal of Advanced Robotic Systems*, vol. 22, no. 2, pp. 1–9, 2025. https://doi.org/10.1177/17298806241312786

[54] A. Alshehri, M. M. Badr, M. Baza, and H. Alshahrani, "Deep Anomaly Detection Framework utilizing federated Learning for electricity theft Zero-Day Cyberattacks," *Sensors*, vol. 24, no. 10, pp. 1–19, 2024. https://doi.org/10.3390/s24103236

[55] H. Shahinzadeh, S. Azani, A. Baghernezhad, S. Mehrabani-Najafabadi, G. B. Gharehpetian, and F. Jurado, "Cyber Threats and Resilience in Smart Grids and Microgrids: A Cybersecurity Perspective on Challenges and Innovations," 2024 19th Iranian Conference on Intelligent Systems (ICIS), Sirjan, Iran, Islamic Republic of, 23-24 October 2024, pp. 299–308. https://doi.org/10.1109/icis64839.2024.10887512

[56] M. Albanese, and M. Varlese, "Smart grids: Impacts and challenges on energy sector, "*Journal of Applied Economic Sciences*, vol. 4, no. 86, pp. 499–510, 2024. https://doi.org/10.57017/jaes.v19.4(86).12

[57] A. F. Yeddou, A. Belouchrani, and A. Mokrane, "Enhancing Peer-to-Peer Energy Trading in Smart Grids through Blockchain Interoperability Using Layer Zero," 2024 6th International Conference on Blockchain Computing and Applications (BCCA), Dubai, United Arab Emirates, 26-29 November 2024, pp. 624–629. https://doi.org/10.1109/bcca62388.2024.10844405

[58] A. S. Aliero, and N. Malhotra, "Application of machine and deep learning models in smart grid functionalities: a survey," *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 11, pp. 679–686, 2024. https://www.irjet.net/archives/V11/i11/IRJET-V11I1103.pdf

[59] M. R. Zaman, M. A. Halim, M. Y. A. Khan, S. Ibrahim, and A. Haque, "Integrating Micro and Smart Grid-Based Renewable Energy Sources with the National Grid in Bangladesh - A Case Study," *Control Systems and Optimization Letters*, vol. 2, no. 1, pp. 75–81, 2024. https://doi.org/10.59247/csol.v2i1.76

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[60] E. H. Sadiq, Y. M. Ameen, H. M. Taha, and N. J. Faqishafyee, "Challenges and Opportunities in Implementing smart grid Technologies in Kurdistan: A Comprehensive review," *Journal of Industrial Intelligence*, vol. 2, no. 2, pp. 94–105, 2024. https://doi.org/10.56578/jii020203

[61] W. Velasquez, G. Z. Moreira-Moreira, and M. S. Alvarez-Alvarado, "Smart Grids Empowered by Software-Defined Network: A Comprehensive review of advancements and challenges," *IEEE Access*, vol. 12, pp. 63400–63416, 2024. https://doi.org/10.1109/access.2024.3396402

[62] N. Xu, Z. Tang, C. Si, J. Bian, and C. Mu, "A review of Smart Grid Evolution and Reinforcement Learning: applications, challenges and future directions," *Energies*, vol. 18, no. 7, pp. 1–19, 2025. https://doi.org/10.3390/en18071837

[63] A. A. Elshazly, I. Elgarhy, A. T. Eltoukhy, M. Mahmoud, W. Eberle, M. Alsabaan, and T. Alshawi, "False data injection attacks on reinforcement Learning-Based charging coordination in smart grids and a countermeasure," *Applied Sciences*, vol. 14, no. 23, pp. 1–23, 2024. https://doi.org/10.3390/app142310874

[64] R. A. Salam, N. I. Ratyal, U. Ahmed, I. Aziz, M. Sajid, and A. Mahmood, "An overview of recent wireless technologies for IoT-Enabled smart grids," *Journal of Electrical and Computer Engineering*, vol. 2024, no. 1, pp. 1–22, 2024. https://doi.org/10.1155/jece/2568751

[65] H. M. D. M. Herath, N. A. Weerasekara, and K. L. D. P. Perera, "An Extensive Review of Smart Grid Technology: Enhancing Energy Efficiency and Reliability," *Journal of Research Technology & Engineering*, vol. 5, no. 4, pp. 169–202, 2024.

[66] M. S. Abdalzaher, M. Shaaban and R. Aburukba, "Leveraging Machine Learning for SCADA-based Smart Grids Security," 2024 8th International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM), Medan, Indonesia, 21-22 November 2024, pp. 141-145, doi: 10.1109/ELTICOM64085.2024.10865372.

[67] N. Barsha, and N. Hubballi, "Anomaly Detection in SCADA Systems: A State Transition Modeling," *IEEE Transactions on Network and Service Management*, vol. 21, pp. 3511-3521, 2024. https://doi.org/10.1109/TNSM.2024.3373881

[68] W. Abdelfattah, A. Abdelhamid, H. Hasanien, and B. Rashad, "Smart Vehicle-to-Grid Integration Strategy for Enhancing Distribution System Performance and Electric Vehicle Profitability," *Energy*, vol. 302, pp. 131807, 2024. https://doi.org/10.1016/j.energy.2024.131807

[69] S. Wali, M. Hannan, P. Ker, S. Rahman, K. Le, R. Begum, S. Tiong, and T. Mahlia, "Grid-connected lithium-ion battery energy storage system towards sustainable energy: A patent landscape analysis and technology updates," *Journal of Energy Storage*, vol. 77, pp. 109986, 2024. https://doi.org/10.1016/j.est.2023.109986

[70] K. Morrissey, P. Dambrauskas, R. MacDonald and G. Ault, "Advanced analytics extending network capacity access in operational DERMS," CIRED 2024 Vienna Workshop, Vienna, Austria, 19-20 June 2024, pp. 841-845, doi: 10.1049/icp.2024.2005.

[71] Y. Shen, Q. Zhou, Y. Wen, Z. Shuai, and Z. Shen, "Integrated Satellite-Terrestrial Network Framework for Next Generation Smart Grid," *IEEE Transactions on Smart Grid*, vol. 15, pp. 5249-5252, 2024. https://doi.org/10.1109/TSG.2024.3424150

[72] H. Naiho, O. Layode, G. Adeleke, E. Udeh, and T. Labake, "Addressing cybersecurity challenges in smart grid technologies: Implications for sustainable energy infrastructure," *Engineering Science & Technology Journal*, vol. 5, no. 6, pp. 1995-2015, 2024. https://doi.org/10.51594/estj.v5i6.1218

[73] T. Deokar, J. Shinde, and R. Sairise, "Artificial Intelligence in Smart Grid Systems: A Comprehensive Review of Machine Learning and Deep Learning Applications," *ShodhKosh: Journal of Visual and Performing Arts*, vol. 5, no. 6, pp. 1506–1514, 2024. https://doi.org/10.29121/shodhkosh.v5.i6.2024.4825

[74] H. Taherdoost, "A Systematic Review of Big Data Innovations in Smart Grids," *Results in Engineering*, vol. 22, pp. 1-13, 2024. https://doi.org/10.1016/j.rineng.2024.102132

[75] D. M. Azizah, and C. Oktavia, "Implementing Blockchain Technology for Securing IoT-Based Smart Grids," *International Journal of Electrical Engineering, Mathematics and Computer Science*, vol. 1, no. 1, pp. 09–12, 2024. https://doi.org/10.62951/ijeemcs.v1i1.70

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[76] M. Tatiya, A. Verma, S. Talekar, S. Kumar, V., B. Kiran, and S. Kumar, "Cybersecurity in IoT-Based Smart Grids: A Comprehensive Survey," *Computer Fraud and Security*, vol. 2024, no. 8, pp. 73-81, 2024. https://doi.org/10.52710/cfs.51

[77] X. Wang, S. Li, and M. Rahman, "A Comprehensive Survey on Enabling Techniques in Secure and Resilient Smart Grids," *Electronics*, vol. 13, no. 11, pp. 1-24, 2024. https://doi.org/10.3390/electronics13112177

[78] M. Ajith, M. Ajith, P. Anil, V. V. Pavithran, and K. K. Mumina, "Smart grid integration using IoT," *International Journal for Research in Applied Science and Engineering Technology*, vol. 13, no. 2, pp. 627–631, 2025. https://doi.org/10.22214/ijraset.2025.66933

[79] M. Khalid, "Smart grids and renewable energy systems: Perspectives and grid integration challenges," *Energy Strategy Reviews*, vol. 51, pp. 1-26, 2024. https://doi.org/10.1016/j.esr.2024.101299

[80] H. Zheng, "Research On Low-Carbon Development Path of New Energy Industry Under the Background of Smart Grid," Journal of King Saud University - Science, vol. 36, no. 3, pp. 103105, 2024. https://doi.org/10.1016/j.jksus.2024.103105

[81] S. Edirisinghe, A. Wijethunge, and C. Ranaweera, "Wi-Fi 6-based home area network for demand response in smart grid," *International Journal of Communication Systems*, vol. 37, no. 9, pp. e5775, 2024. https://doi.org/10.1002/dac.5775

[82] Y. Tang, Y. Zhang, T. Niu, Z. Li, Z. Zhang, H. Chen, and L. Zhang, "A survey on Blockchain-Based Federated Learning: Categorization, Application and analysis," *Computer Modeling in Engineering & Sciences*, vol. 139, no. 3, pp. 2451–2477, 2024. https://doi.org/10.32604/cmes.2024.030084

[83] B. Goswami, Y. Tian, Y. Mishra, J. Jin, and Y. Tang, "Communication Solutions for the Last Mile of Smart Grid: Neighborhood Area Networks in Smart Grid Communications: Standards and Challenges," *IEEE Power and Energy Magazine*, vol. 22, pp. 118-133, 2024. https://doi.org/10.1109/MPE.2024.3386652

[84] B. Goswami, R. Jurdak, and G. Nourbakhsh, "Node Allocation Strategy for Low Latency Neighborhood Area Networks in Smart Grid," *IEEE Transactions on Network Science and Engineering*, vol. 11, pp. 5087-5098, 2024. https://doi.org/10.1109/TNSE.2024.3427840

[85] M. Boeding, P. Scalise, M. Hempel, H. Sharif, and J. Lopez, "Toward Wireless Smart Grid Communications: An Evaluation of Protocol Latencies in an Open-Source 5G Testbed," *Energies*, vol. 17, no. 2, pp. 1-18, 2024. https://doi.org/10.3390/en17020373

[86] H. Huang, L. Cheng, Z. Yu, W. Zhang, Y. Mu, and K. Xu, "Optical Fiber Communication System Based on Intelligent Joint Source-Channel Coded Modulation," *Journal of Lightwave Technology*, vol. 42, pp. 2009-2017, 2024. https://doi.org/10.1109/JLT.2023.3328311

[87] A. L. Challoob, "Data transfer in smart grids: Leveraging MIMO-OFDM for enhanced communication," *International Journal of Computational and Electronic Aspects in Engineering*, vol. 5, no. 4, pp. 154–164, 2024. https://doi.org/10.26706/ijceae.5.4.20241104

[88] S. Simonthomas, R. Subramanian, and S. A. Mathiew, "A Survey of Enhancing Cyber Physical System Security in Smart grid," 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT), 209, Chennai, India, 17-18 April 2024, pp. 1–6. https://doi.org/10.1109/ic3iot60841.2024.10550307

[89] K. A. Abdulsalam, J. Adebisi, M. Emezirinwune, and O. Babatunde, "An overview and multicriteria analysis of communication technologies for smart grid applications," *e-Prime - Advances in Electrical Engineering Electronics and Energy*, vol. 3, pp. 1–16, 2023. https://doi.org/10.1016/j.prime.2023.100121

[90] J. C. Rodríguez, F. Grijalva, M. García, D. E. C. Barragán, B. A. A. Acurio, and H. Carvajal, "Wireless Communication Technologies for Smart Grid Distribution Networks," *Engineering Proceedings*, vol. 47, no. 1, pp. 1–15, 2023. https://doi.org/10.3390/engproc2023047007

[91] J. Kim, J. Kim, and J. Lee, "Efficient Cluster Tree Topology Operation and Routing for IEEE 802.15.4-Based Smart Grid Networks," *Sensors*, vol. 23, no. 13, pp. 1-26, 2023. *https://doi.org/10.3390/s23135950*

[92] M. Sheba, D. Mansour, and N. Abbasy, "A new low-cost and low-power industrial internet of things infrastructure for effective integration of distributed and isolated systems with smart grids," *IET Generation, Transmission & Distribution*, vol. 17, no. 20, pp. 4554-4573, 2023. https://doi.org/10.1049/gtd2.12951

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[93] M. D. Hossain, H. Ochiai, L. Khan and Y. Kadobayashi, "Smart Meter Modbus RS-485 Intrusion Detection by Federated Learning Approach," 2023 15th International Conference on Computer and Automation Engineering (ICCAE), Sydney, Australia, 03-05 March 2023, pp. 559-564, doi: 10.1109/ICCAE56788.2023.10111132.

[94] S. Maneria and K. K. Pramanik, "IoT Narrow Band for Smart Grid," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 12-13 May 2023, pp. 2260-2266, doi: 10.1109/ICACITE57410.2023.10182757

[95] A. A. Bisu, H. Sun and A. Gallant, "Integrated Satellite-Terrestrial Network for Smart Grid Communications in 6G Era," 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 06-08 January 2025, pp. 01044-01049, doi: 10.1109/CCWC62904.2025.10903893

[96] G. Koulouras, S. Katsoulis, and F. Zantalis, "Evolution of Bluetooth Technology: BLE in the IoT Ecosystem," *Sensors*, vol. 25, no. 4, pp. 1-37, 2025. https://doi.org/10.3390/s25040996

[97] D. Li, Q. Yang, F. Zhang, Y. Wang, Y. Qian, and D. An, "Research on Privacy Issues in Smart Metering System: An Improved TCN-Based NILM Attack Method and Practical DRL-Based Rechargeable Battery Assisted Privacy Preserving Method," *IEEE Transactions on Automation Science and Engineering*, vol. 21, pp. 2882-2899, 2024. https://doi.org/10.1109/TASE.2023.3270543

[98] S. S. Reka, T. Dragicevic, P. Venugopal, V. Ravi, and M. K. Rajagopal, "Big Data Analytics and Artificial Intelligence aspects for privacy and security concerns for Demand Response Modelling in Smart Grid: A Futuristic Approach," *Heliyon*, vol. 10, no. 15, pp. 1–13, 2024. https://doi.org/10.1016/j.heliyon.2024.e35683

[99] K. Bhatia, and S. S. Ojha, "Federated Learning Framework for Early Detection of Reconnaissance Attacks in Smart Grid Environments," 2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, India, 15-16 March 2024, pp. 1–6. https://doi.org/10.1109/dicct61038.2024.10533039

[100] M. A. Khan, A. M. Saleh, M. Waseem, and V. István, "Smart Grid Cyber Attacks: Overview, Threats, And Countermeasures," 2024 22nd International Conference on Intelligent Systems Applications to Power Systems (ISAP), Budapest, Hungary, 16-19 September 2024, pp. 1–5. https://doi.org/10.1109/isap63260.2024.10744349

[101] M. Alghassab, "Investigating the Progress of Smart Grid Technologies in the Kingdom of Saudi Arabia: Emerging Trends and Challenges," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 14-16 September 2023, pp. 326–331. https://doi.org/10.1109/ic3i59117.2023.10397775

[102] V. Pritish, P. Kumar, K. Annapurani, and A. Choudhary, "Cybersecurity strategies for protecting smart grid in Residential building complex from attacks," 2024 2nd International Conference on Advancements and Key Challenges in Green Energy and Computing (AKGEC), Ghaziabad, India, 21-23 November 2024, pp. 1–6. https://doi.org/10.1109/akgec62572.2024.10868067

[103] M. Khalaf, A. Ayad, M. H. K. Tushar, M. Kassouf, and D. Kundur, "A survey on Cyber-Physical Security of active distribution networks in smart Grids," *IEEE Access*, vol. 12, pp. 29414–29444, 2024. https://doi.org/10.1109/access.2024.3364362

[104] A. Salehpour, and I. Al-Anbagi, "RTAP: A real-time model for attack detection and prediction in smart grid systems," *IEEE Access*, vol. 12, pp. 130425–130443, 2024. https://doi.org/10.1109/access.2024.3458874

[105] M. Usama, and M. N. Aman, "Command injection attacks in smart grids: a survey," *IEEE Open Journal of Industry Applications*, vol. 5, pp. 75–85, 2024. https://doi.org/10.1109/ojia.2024.3365576

[106] L. Nguyen, V. Nguyen, R. Hwang, J. Kuo, Y. Chen, C. Huang, and P. Pan, "Towards Secured Smart Grid 2.0: Exploring security threats, protection models, and challenges," *IEEE Communications Surveys & Tutorials*, pp. 1-39, 2024. https://doi.org/10.1109/comst.2024.3493630

[107] D. Agnew, S. Boamah, A. Bretas, and J. McNair, "Network Security Challenges and Countermeasures for Software-Defined Smart Grids: A survey," *Smart Cities*, vol. 7, no. 4, pp. 2131–2181, 2024. https://doi.org/10.3390/smartcities7040085

[108] A. Rastogi, A. Agrawal, R. Singh, and A. Aggarwal, "A Comprehensive Cybersecurity Resilience Framework Augmenting Smart Grid Stability. 2024 IEEE 5th India Council International Subsections Conference

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

(INDISCON), Chandigarh, India, 22-24 August 2024, pp. 1–6. https://doi.org/10.1109/indiscon62179.2024.10744380

[109] M. S. Sujatha, S. S. Banu, V. S. Sriyesh, G. Sreenivasan, M. Kuruba, and M. G. M. Reddy, "Cyber Security for Power System. 2024 10th International Conference on Electrical Energy Systems (ICEES), Chennai, India, 22-24 August 2024, pp. 1–5. https://doi.org/10.1109/icees61253.2024.10776829

[110] R. Alajlan, M. M. H. Rahman, M. Alnaeem, and M. Almaiah, "A Literature Review on Cybersecurity Risks and Challenges Assessments in Virtual Power Plants: Current landscape and future research Directions," *IEEE Access*, vol. 12, pp. 188813-188827, 2024. https://doi.org/10.1109/access.2024.3515635

[111] D. Tang, J. M. Guerrero, and E. Zio, "Securing demand–response in smart grids against false pricing attacks," *Energy Reports*, vol. 12, pp. 892–905, 2024. https://doi.org/10.1016/j.egyr.2024.06.068

[112] Y. Wu, H. Guo, Y. Han, S. Li, and J. Liu, "A Security-Enhanced Authentication and Key Agreement Protocol in Smart Grid," *IEEE Transactions on Industrial Informatics*, vol. 20, pp. 11449-11457, 2024. https://doi.org/10.1109/TII.2024.3399915

[113] A. Umar, D. Kumar, T. Ghose and M. A. Rahman, "Securing Smart Grids with Blockchain: Enhancing Data Integrity and Automated Access Control," 2024 IEEE 11th Power India International Conference (PIICON), JAIPUR, India, 10-12 December 2024, pp. 1-6, doi: 10.1109/PIICON63519.2024.10995102.

[114] X. Ai, Y. Dong, Y. Huang, Q. Meng, F. Teng, Y. Yin, and Z. Cao, "Secure Sharing and Integrity Assurance of Data in Smart Grids," 2024 Sixth International Conference on Next Generation Data-driven Networks (NGDN), Shenyang, China, 26-28 April 2024, pp. 322-327, doi: 10.1109/NGDN61651.2024.10744157.

[115] M. S. Qureshi, I. Ullah Khan and K. Kim, "Securing the Smart Grid: A Comprehensive Analysis of Recent Cyber Attacks," 2023 5th International Conference on Electrical, Control and Instrumentation Engineering (ICECIE), Kuala Lumpur, Malaysia, 22-24 December 2023, pp. 1-6, doi: 10.1109/ICECIE58751.2024.10457427.

[116] S. Roy, A. Kumar, and U. P. Rao, "Security Attacks and it's Countermeasures on Smart Grid: A Review," 2023 International Conference on Computer, Electronics & Electrical Engineering & Their Applications (IC2E3), Srinagar Garhwal, India, 08-09 June 2023, pp. 1–6. https://doi.org/10.1109/ic2e357697.2023.10262686

[117] K. A. Mutlaq, V. O. Nyangaresi, M. A. Omar, Z. A. Abduljabbar, I. Q. Abduljaleel, J. Ma, and M. A. A. Sibahee, "Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance," PLoS ONE, vol. 19, no. 1, pp. 1–31, 2024. https://doi.org/10.1371/journal.pone.0296781

[118] K. Prateek, S. Maity, and R. Amin, "An Unconditionally Secured Privacy-Preserving Authentication Scheme for Smart Metering Infrastructure in Smart Grid," *IEEE Transactions on Network Science and Engineering*, vol. 10, pp. 1085-1095, 2023. https://doi.org/10.1109/TNSE.2022.3226902

[119] S. Choudhary, A. Kumar, K. Berwal and M. Pundir, "Securing Smart Grid: A Cloud-Assisted Approach with Multi-Authority Attribute-Based Encryption," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 24-28 June 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10724170

[120] M. Badra, and R. Borghol, "An efficient blockchain-based privacy preservation scheme for smart grids," *Frontiers in Communications and Networks*, vol. 6, pp. 1-11, 2025. https://doi.org/10.3389/frcmn.2025.1584152

[121] G. Indiravathi, M. P. Kumar, A. Usha, R. Kumar, T. Lohith and S. Shahid, "Enhancing Data Privacy and Accountability in Smart Grids with Blockchain Technology," 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT), Greater Noida, India, 29-31 August 2024, pp. 1-6, doi: 10.1109/ICEECT61758.2024.10739131.

[122] F. Salem, R. Khairy, and I. Ali, "An elliptic curve-based lightweight mutual authentication scheme for secure communication in smart grids," *International Journal of Information Technology*. 2024. https://doi.org/10.1007/s41870-024-01813-1

[123] A. Aghajari, T. Niknam, S. Sharifhosseini, M. Taabodi, and M. Pourbehzadi, "Enhanced resilience in smart grids: A neural network-based detection of data integrity attacks using improved war strategy optimization," *Electric Power Systems Research*, vol. 239, pp. 111249, 2025. https://doi.org/10.1016/j.epsr.2024.111249

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[124] G. Ali, A. Thomas, M. M. Mijwil, K. Al-Mahzoum, M. Sallam, A. O. Salau, I. Adamopoulos, I. Bala, and A. Y. R. Al-jubori, "Blockchain and Federated Learning in Edge-Fog-Cloud Computing Environments for Smart Logistics," *Mesopotamian Journal of CyberSecurity*, vol. 5, no, 2, pp. 735–769, 2025. https://doi.org/10.58496/

[125] X. Wang, Q. Yu, D. Lv, T. Yang, Y. Wei, L. Liu, P. Zhang, Y. Zhang, and W. Zhang, "Dynamic spectrum sharing based on federated learning in smart grids and power communication networks," *IET Communications*, vol. 19, no. 1, pp. 1–8, 2025. https://doi.org/10.1049/cmu2.12766

[126] M. A. Khan, "Enhancing Grid Resilience Entangled with Federated Learning for Secure Data Aggregation in Smart Grids," 2025 27th International Conference on Advanced Communications Technology (ICACT), Pyeong Chang, Korea, Republic of, 16-19 February 2025, pp. 234–240. https://doi.org/10.23919/icact63878.2025.10936689

[127] S. M. Rajagopal, S. Supriya, and R. Buyya, "Blockchain Integrated Federated Learning in Edge-Fog-Cloud Systems for IoT-based Healthcare Applications: A Survey," arXiv (Cornell University), pp. 1–32, 2024. https://doi.org/10.48550/arxiv.2406.05517

[128] P. Liu, L. Jia, and Y. Xiao, "Participant selection for efficient and trusted federated learning in Blockchain-Assisted hierarchical federated learning architectures," *Future Internet*, vol. 17, no. 2, pp. 1–19, 2025. https://doi.org/10.3390/fi17020075

[129] A. A. Elshazly, I. Elgarhy, M. Mahmoud, M. I. Ibrahem, and M. Alsabaan, "A Privacy-Preserving RL-Based secure charging coordinator using efficient FL for smart grid home batteries," *Energies*, vol. 18, no. 4, pp. 1–34, 2025. https://doi.org/10.3390/en18040961

[130] O. O'Connor, and T. Elfouly, "Federated Learning: A Paradigm Shift in Cybersecurity for Smart Grids," 2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Knoxville, TN, USA, 01-03 July 2024, pp. 821–824. https://doi.org/10.1109/isvlsi61997.2024.00163

[131] S. Shao, Y. Wang, C. Yang, Y. Liu, X. Chen, and F. Qi, "WFB: watermarking-based copyright protection framework for federated learning model via blockchain," *Scientific Reports*, vol. 14, no. 1, pp. 1–16, 2024. https://doi.org/10.1038/s41598-024-70025-1

[132] X. Deng, T. Ma, H. Li, and M. Lu, "Federated Large Language Models for Smart Grid: A Communication Efficient LORA approach," 2024 IEEE 4th International Conference on Civil Aviation Safety and Information Technology (ICCASIT), Hangzhou, China, 23-25 October 2024, pp. 1369–1374. https://doi.org/10.1109/iccasit62299.2024.10827901

[133] Z. N. Limbepe, K. Gai, and J. Yu, "Blockchain-Based Privacy-Enhancing Federated Learning in smart Healthcare: a survey," *Blockchains*, vol. 3, no. 1, pp. 1–38, 2025. https://doi.org/10.3390/blockchains3010001

[134] H. Mei, C. Deng, H. Liu, Y. Zeng, and Y. Zeng, "Application of Federated Learning in Smart Grid Fault Diagnosis: Privacy Protection and Efficiency Improvement," 2024 6th International Conference on Energy, Power and Grid (ICEPG), Guangzhou, China, 27-29 September 2024, pp. 743–746. https://doi.org/10.1109/icepg63230.2024.10775979

[135] P. K. Myakala, C. Bura, and A. K. Jonnalagadda, "Federated Learning and Data Privacy: A review of Challenges and opportunities," *International Journal of Research Publication and Reviews*, vol. 5, no. 12, pp. 1867–1879, 2024. https://doi.org/10.55248/gengpi.5.1224.3512

[136] C. Papadopoulos, K. Kollias, and G. F. Fragulis, "Recent advancements in federated learning: state of the art, fundamentals, principles, IoT applications and future trends," *Future Internet*, vol. 16, no. 11, pp. 1–41, 2024. https://doi.org/10.3390/fi16110415

[137] A. H. Bondok, M. M. Badr, M. Mahmoud, A. T. El-Toukhy, M. Alsabaan, F. Amsaad, and M. I. Ibrahem, "A Trojan Attack against Smart Grid Federated Learning and Countermeasures," *IEEE Access*, vol. 12, pp. 191828–191846, 2024. https://doi.org/10.1109/access.2024.3515099

[138] H. Zahid, A. Zulfiqar, M. Adnan, S. Iqbal, and S. E. G. Mohamed, "A review on Socio-technical Transition Pathway to European Super Smart Grid: Trends, challenges and Way forward via Enabling Technologies," *Results in Engineering*, vol. 25, pp. 1–28, 2025. https://doi.org/10.1016/j.rineng.2025.104155

[139] T. Manoj, K. Makkithaya, and V. G. Narendra, "A Blockchain-Assisted trusted federated learning for smart agriculture," *SN Computer Science*, vol. 6, no. 3, pp. 1–26, 2025. https://doi.org/10.1007/s42979-025-03672-4

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[140] M. Sarker, B. Shanmugam, S. Azam, and S. Thennadil, "Enhancing smart grid load forecasting: An attention-based deep learning model integrated with federated learning and XAI for security and interpretability," *Intelligent Systems with Applications*, vol. 23, pp. 1-17, 2024. https://doi.org/10.1016/j.iswa.2024.200422

[141] H. Manzoor, A. Shabbir, A. Chen, D. Flynn, and A. Zoha, "A Survey of Security Strategies in Federated Learning: Defending Models, Data, and Privacy," *Future Internet*, vol. 16, no. 10, pp. 1-37, 2024. https://doi.org/10.3390/fi16100374

[142] A. Shabbir, H. Manzoor, M. Manzoor, S. Hussain, and A. Zoha, "Robustness Against Data Integrity Attacks in Decentralized Federated Load Forecasting," *Electronics*, vol. 13, no. 23, pp. 1-23, 2024. https://doi.org/10.3390/electronics13234803

[143] A. Shabbir, H. U. Manzoor, R. A. Ahmed and Z. Halim, "Resilience of Federated Learning Against False Data Injection Attacks in Energy Forecasting," 2024 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), Miri Sarawak, Malaysia, 17-19 January 2024, pp. 245-249, doi: 10.1109/GECOST60902.2024.10475064

[144] S. Shafi, N. Tariq, F. Khan, and A. Ali, "Federated Learning for Enhanced Malware Threat Detection to Secure Smart Power Grids," Proceedings of the International Conference on Ubiquitous Computing and Ambient Intelligence, Belfast, United Kingdom, 27-29 November 2024, pp. 692-703. https://doi.org/10.1007/978-3-031-77571-0_66

[145] M. Mohammadi, R. Shrestha, and S. Sinaei, "Integrating Federated Learning and Differential Privacy for Secure Anomaly Detection in Smart Grids," Proceedings of the 2024 8th International Conference on Cloud and Big Data Computing, Oxford, United Kingdom, 15 - 17 August 2024, pp. 60 - 66. https://doi.org/10.1145/3694860.3694869

[146] D. Perdigão, T. Cruz, P. Simões, and P. H. Abreu, "Data-Centric Federated Learning for Anomaly Detection in Smart Grids and Other Industrial Control Systems," NOMS 2024-2024 IEEE Network Operations and Management Symposium, Seoul, Korea, Republic of, 06-10 May 2024, pp. 1–5. https://doi.org/10.1109/noms59830.2024.10574962

[147] M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain and Federated Reinforcement Learning for Vehicle-to-Everything Energy Trading in Smart Grids," *IEEE Transactions on Artificial Intelligence*, vol. 5, pp. 839-853, 2024. https://doi.org/10.1109/TAI.2023.3262597

[148] R. S. S. Nuvvula, P. P. Kumar, P. Akki, S. R. Ahammed, J. R. Sudheer, R. Hushein, and A. Ali, "Federated Learning-Based Energy Forecasting and Trading Platform for Decentralized Renewable Energy Markets," 2024 12th International Conference on Smart Grid (icSmartGrid), Setubal, Portugal, 27-29 May 2024, pp. 277-283, doi: 10.1109/icSmartGrid61824.2024.10578121

[149] H. Ma, H. Zhang, D. Tian, D. Yue, and G. P. Hancke, "Optimal demand response based dynamic pricing strategy via Multi-Agent Federated Twin Delayed Deep Deterministic policy gradient algorithm," *Engineering Applications of Artificial Intelligence*, vol. 133, pp. 108012, 2024. https://doi.org/10.1016/j.engappai.2024.108012

[150] W. Zhang, and Y. Li, "Aggregator-Grid Interactive Building Dual-Layer Price-Responsive Demand Response Scheduling Based on Federated Deep Reinforcement Learning," *IEEE Transactions on Smart Grid*, vol. 16, pp. 1142-1154, 2025. https://doi.org/10.1109/TSG.2024.3458074

[151] I. Rustambekov, G. S. Saidakhmedovich, B. Abduvaliyev, E. Kan, I. Abdukhakimov, M. Yakubova, and D. Karimov, "Predictive Maintenance of Smart Grid Components Based on Real-Time Data Analysis," 2024 6th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA), Lipetsk, Russian Federation, 13-15 November 2024, pp. 949-952, doi: 10.1109/SUMMA64428.2024.10803838

[152] A. A. Hassna, M. Fatima, K. Abdellatif and E. K. Mohammed, "Federate learning for Solar Power Forecasting in smart cities," GLOBECOM 2024 - 2024 IEEE Global Communications Conference, Cape Town, South Africa, 08-12 December 2024, pp. 3721-3726, doi: 10.1109/GLOBECOM52923.2024.10901217.

[153] S. Pokhrel, M. Hossain, and A. Walid, "Modeling Practically Private Wireless Vehicle to Grid System With Federated Reinforcement Learning," *IEEE Transactions on Services Computing*, vol. 17, pp. 1044-1055, 2024. https://doi.org/10.1109/TSC.2023.3344460

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[154] S. Danish, A. Hameed, A. Ranjha, G. Srivastava, and K. Zhang, "Block-FeDL: Electric Vehicle Charging Load Forecasting Using Federated Learning and Blockchain," *IEEE Transactions on Vehicular Technology*, vol. 74, pp. 2048-2056, 2025. https://doi.org/10.1109/TVT.2024.3406946

[155] M. Khan, M. Farooq, M. Saleem, T. Shahzad, M. Ahmad, S. Abbas, and A. Abu-Mahfouz, "Smart buildings: Federated learning-driven secure, transparent and smart energy management system using XAI," *Energy Reports*, vol. 13, pp. 2066-2081, 2025. https://doi.org/10.1016/j.egyr.2025.01.063

[156] Y. Lin, Y. Chen, and S. Wei, "Active Privacy-Preserving, Distributed Edge–Cloud Orchestration–Empowered Smart Residential Mains Energy Disaggregation in Horizontal Federated Learning," *International Transactions on Electrical Energy Systems*, vol. 2025, no. 1, pp. 2556622, 2025. https://doi.org/10.1155/etep/2556622

[157] C. Ren, H. Yu, R. Yan, Q. Li, Y. Xu, D. Niyato, and Z. Dong, "SecFedSA: A Secure Differential-Privacy-Based Federated Learning Approach for Smart Cyber–Physical Grid Stability Assessment,: IEEE Internet of Things Journal, vol. 11, pp. 5578-5588, 2024. https://doi.org/10.1109/JIOT.2023.3308170

[158] M. Massaoudi, H. Abu-Rub, and A. Ghrayeb, "FLACON: A Deep Federated Transfer Learning-Enabled Transient Stability Assessment During Symmetrical and Asymmetrical Grid Faults," *IEEE Open Journal of Industry Applications*, vol. 5, pp. 253-266, 2024. https://doi.org/10.1109/OJIA.2024.3426281

[159] S. Salim, N. Moustafa, and B. Turnbull, "BFL-SC: A blockchain-enabled federated learning framework, with smart contracts, for securing social media-integrated internet of things systems," *Ad Hoc Networks*, pp. 1–13, 2025. https://doi.org/10.1016/j.adhoc.2025.103760

[160] H. A. Ahmed, H. M. Jasim, A. N. Gatea, A. A. A. Al-Asadi, and H. A. A. Al-Asadi, "A secure and efficient blockchain enabled federated Q-learning model for vehicular Ad-hoc networks," *Scientific Reports*, vol. 14, no. 1, pp. 1–24, 2024. https://doi.org/10.1038/s41598-024-82585-3

[161] A. Sharma, and N. Marchang, "A review on client-server attacks and defenses in federated learning," *Computers & Security*, vol. 140, pp. 103801, 2024. https://doi.org/10.1016/j.cose.2024.103801

[162] Q. Han, S. Lu, W. Wang, H. Qu, J. Li, and Y. Gao, "Privacy preserving and secure robust federated learning: A survey," *Concurrency and Computation: Practice and Experience*, vol. 36, no. 13, pp. e8084, 2024. https://doi.org/10.1002/cpe.8084

[163] Z. Xie, and Z. Li, "A Blockchain Multi-Chain federated learning framework for enhancing security and efficiency in intelligent unmanned ports," *Electronics*, vol. 13, no. 24, pp. 1–18, 2024. https://doi.org/10.3390/electronics13244926

[164] W. Almutairi, and T. Moulahi, "Joining Federated Learning to Blockchain for digital forensics in IoT," *Computers*, vol. 12, no. 8, pp. 1–16, 2023. https://doi.org/10.3390/computers12080157

[165] H. Belfqih, and A. Abdellaoui, "Decentralized Blockchain-Based Authentication and Interplanetary File System-Based data Management Protocol for Internet of Things using ASCON," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, pp. 1–22, 2025. https://doi.org/10.3390/jcp5020016

[166] O. S. Igonor, M. B. Amin, and S. Garg, "The Application of Blockchain Technology in the field of Digital Forensics: A literature review," *Blockchains*, vol. 3, no. 1, pp. 1–46, 2025. https://doi.org/10.3390/blockchains3010005

[167] K. S. Kumar, J. A. Alzubi, N. Sarhan, E. M. Awwad, V. Kandasamy, and G. Ali, "A secure and efficient BlockChain and distributed Ledger technology-based optimal resource management in digital twin beyond 5G networks using hybrid energy valley and levy Flight Distributer Optimization algorithm," *IEEE Access*, vol. 12, pp. 110331–110352, 2024. https://doi.org/10.1109/access.2024.3435847

[168] A. Denis, A. Thomas, W. Robert, A. Samuel, S. P. Kabiito, Z. Morish, M. Sallam, G. Ali, and M. M. Mijwil, "A Survey on Artificial Intelligence and Blockchain Applications in Cybersecurity for Smart Cities," *SHIFRA*, vol. 2025, pp. 1-45, 2025. https://doi.org/10.70470/SHIFRA/2025/001

[169] G. Ali, S. Aziku, S. P. Kabiito, M. Zaward, T. Adebo, R. Wamusi, D. Asiku, M. Sallam, M. M. Mijwil, J. Ayad, A. O. Salau, and K. Dhoska, "Integration of Artificial Intelligence, Blockchain, and Quantum Cryptography for Securing the Industrial Internet of Things (IIoT): Recent Advancements and Future Trends," *Applied Data Science and Analysis*, vol. 2025, pp. 19–82, 2025. https://doi.org/10.58496/ADSA/2025/004

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[170] C. Regueiro, S. De Diego, and B. Urkizu, "Leveraging blockchain technology for secure 5G offloading processes," *Future Internet*, vol. 17, no. 5, pp. 1–32, 2025. https://doi.org/10.3390/fi17050197

[171] S. Eivazzadeh, S. Mutyala, J. Chinthala, F. Fotrousi, and S. Khatibi, "Blockchains' Impact on Enhancing Physical Activity, Rehabilitation, Sport, and Exercise-Based Therapeutics: A Systematic Review," *Applied Sciences*, vol. 15, no. 7, pp. 1–19, 2025. https://doi.org/10.3390/app15073683

[172] A. Enaya, X. Fernando, and R. Kashef, "Survey of Blockchain-Based Applications for IoT," *Applied Sciences*, vol. 15, no. 8, pp. 1–37, 2025. https://doi.org/10.3390/app15084562

[173] B. Seshasai, E. Koley, and S. Ghosh, "Blockchain for Secure and Decentralized Power System Operation in Smart Grid Systems," 2025 Fourth International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur, India, 20-22 January 2025, pp. 807–811. https://doi.org/10.1109/icpc2t63847.2025.10958672

[174] A. K. Abbas, "Blockchain Technology and Its Issues: Types, Applications, Challenges, and Future Directions," *Journal of Information Systems Engineering and Managemen*t, vol. 10, no. 17s, pp. 103–116, 2025.

[175] N. Singh, V. Mittal, V. Rawat, and P. Kumar, "Blockchain Technology: Reshaping Telemedicine and Telehealth Services for Emergency Management," 2025 International Conference on Pervasive Computational Technologies (ICPCT), Greater Noida, India, 08-09 February 2025, pp. 619–624. https://doi.org/10.1109/icpct64145.2025.10940394

[176] N. R. Pendli, S. Naveen, M. H. Heartlin, R. Kayalvizhi, C. A. Arul, and H. L. Yadav, "Blockchain for Zero-Trust Security Models: A Decentralized Approach to Enterprise Cybersecurity," *Journal of Information Systems Engineering and Management*, vol. 10, no. 33s, pp. 807–813, 2025.

[177] M. Ajaj, and S. Kalash, "Securing the Future of IoT: Exploring the Role of Blockchain Technology in IoT Security," 2025 5th IEEE Middle East and North Africa Communications Conference (MENACOMM), Byblos, Lebanon, 20-22 February 2025, pp. 1–6. https://doi.org/10.1109/menacomm62946.2025.10911025

[178] D. Commey, S. G. Hounsinou, and G. V. Crosby, "Post-Quantum Secure Blockchain-Based federated Learning Framework for healthcare analytics," *IEEE Networking Letters*, pp. 1–4, 2025. https://doi.org/10.1109/lnet.2025.3563434

[179] D. Marchsreiter, "Towards quantum-safe blockchain: Exploration of PQC and public-key recovery on embedded systems," *IET Blockchain*, vol. 5, no. 1, pp. 1–19, 2025. https://doi.org/10.1049/blc2.12094

[180] T. N. A. A. Attar, M. A. Mohammed, and R. N. Mohammed, "Exploring Post-Quantum Cryptography: Evaluating Algorithm Resilience against Global Quantum Threats," UHD Journal of Science and Technology, vol. 9, no. 1, pp. 18–28, 2025. https://doi.org/10.21928/uhdjst.v9n1y2025.pp18-28

[181] P. Chandre, H. Hingoliwala, A. Uttarkar, B. D. Shendkar, D. Lokare, and P. Sontakke, "Post-Quantum Cryptography: Securing Critical Infrastructure Against Emerging Quantum Threats," 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 13-14 December 2024, pp. 1–7. https://doi.org/10.1109/ictbig64922.2024.10911612

[182] K. C. Dekkaki, I. Tasic, and M. Cano, "Exploring Post-Quantum Cryptography: Review and directions for the transition process," *Technologies*, vol. 12, no. 12, pp. 1–23, 2024. https://doi.org/10.3390/technologies12120241

[183] K. Shim, B. Kim, and W. Lee, "Research on quantum key, distribution key and post-quantum cryptography key applied protocols for data science and web security," *Journal of Web Engineering*, vol. 23, no. 6, pp. 813–830, 2024. https://doi.org/10.13052/jwe1540-9589.2365

[184] S. Ahmadunnisa, and S. E. Mathe, "Multi-LFSR architectures for BRLWE-Based post Quantum cryptography," IEEE Access, vol. 12, pp. 96258–96272, 2024. https://doi.org/10.1109/access.2024.3426990

[185] M. Zhang, J. Wang, J. Lai, M. Dong, Z. Zhu, R. Ma, and J. Yang, "Research on development progress and test evaluation of Post-Quantum cryptography," *Entropy*, vol. 27, no. 2, pp. 1–15, 2025. https://doi.org/10.3390/e27020212

[186] S. Kommera, "Quantum-Resistant Cryptography: Preparing for the Post-Quantum Cybersecurity Era," *International Journal of Research in Computer Applications and Information Technology (IJRCAIT)*, vol. 8, no. 1, pp. 1737–1749, 2025. https://doi.org/10.34218/ijrcait_08_01_127

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[187] D. Dziechciarz, and M. Niemiec, "Efficiency analysis of NIST-Standardized Post-Quantum Cryptographic Algorithms for digital signatures in various environments," *Electronics*, vol. 14, no. 1, pp. 1–18, 2024. https://doi.org/10.3390/electronics14010070

[188] G. Fitzgibbon, and C. Ottaviani, "Constrained Device Performance Benchmarking with the Implementation of Post-Quantum Cryptography," *Cryptography*, vol. 8, no. 2, pp. 1–17, 2024. https://doi.org/10.3390/cryptography8020021

[189] P. Rani, A. K. Singh, A. Parashar and D. Saxena, "Quantum-Secure Data Transmission in Smart Grid," 2024 IEEE 17th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), Kuala Lumpur, Malaysia, 16-19 December 2024, pp. 475-481, doi: 10.1109/MCSoC64144.2024.00084.

[190] K. Mansoor, M. Afzal, W. Iqbal, and Y. Abbas, "Securing the future: exploring post-quantum cryptography for authentication and user privacy in IoT devices," *Cluster Computing*, vol. 28, no. 93, 2024. https://doi.org/10.1007/s10586-024-04799-4

[191] M. Naz, W. Elmedany, and M. Ali, "Securing SCADA systems in smart grids with IoT integration: A Self-Defensive Post-Quantum Blockchain Architecture," *Internet Things*, vol. 28, pp. 101381, 2024. https://doi.org/10.1016/j.iot.2024.101381

[192] H. Shekhawat, and D. 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, pp. e8080, 2024. https://doi.org/10.1002/cpe.8080

[193] K. Prateek, M. Das, S. Surve, S. Maity, and R. Amin, "Q-Secure-P²-SMA: Quantum-Secure Privacy- Preserving Smart Meter Authentication for Unbreakable Security in Smart Grid," *IEEE Transactions on Network and Service Management*, vol. 21, pp. 5149-5163, 2024. https://doi.org/10.1109/TNSM.2024.3357103

[194] B. Liu, J. Wu, and L. Chai, "Distributed Privacy-Preserving Algorithm for Economic Dispatch and Demand Response of Smart Grid With Homomorphic Encryption," *IEEE Transactions on Smart Grid*, vol. 16, pp. 173-182, 2025. https://doi.org/10.1109/TSG.2024.3453502

[195] B. Bera and B. Sikdar, "Securing Post-Quantum Communication for Smart Grid Applications," 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Oslo, Norway, 17-20 September 2024, pp. 555-561, doi: 10.1109/SmartGridComm60555.2024.10738045

[196] A. Kalapaaking, I. Khalil, X. Yi, K. Lam, G. Huang, and N. Wang, "Auditable and Verifiable Federated Learning Based on Blockchain-Enabled Decentralization," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 36, pp. 102-115, 2024. https://doi.org/10.1109/TNNLS.2024.3407670

[197] L. Garms, T. Paraïso, N. Hanley, A. Khalid, C. Rafferty, J. Grant, J. Newman, A. Shields, C. Cid, and M. O'Neill, "Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem," *Advanced Quantum Technologies*, vol. 7, no. 4, pp. 2300304, 2024. https://doi.org/10.1002/qute.202300304

[198] A. A. Abdellatif, K. Shaban, and A. Massoud, "Blockchain-enabled distributed learning for enhanced smart grid security and efficiency," *Computers & Electrical Engineering*, vol. 123, pp. 1–14, 2024. https://doi.org/10.1016/j.compeleceng.2024.110012

[199] H. Chen, R. Zhou, Y. Chan, Z. Jiang, X. Chen, and E. Ngai, "LiteChain: A Lightweight Blockchain for Verifiable and Scalable Federated Learning in Massive Edge Networks," *IEEE Transactions on Mobile Computing*, vol. 24, pp. 1928-1944, 2025. https://doi.org/10.1109/TMC.2024.3488746

[200] R. Xiong, W. Ren, S. Zhao, J. He, Y. Ren, K. Choo, and G. Min, "CoPiFL: A collusion-resistant and privacy-preserving federated learning crowdsourcing scheme using blockchain and homomorphic encryption," *Future Generation Computer Systems*, vol. 156, pp. 95-104, 2024. https://doi.org/10.1016/j.future.2024.03.016

[201] K. Venkatesan, and S. Rahayu, "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques," *Scientific Reports*, vol. 14, pp. 1-24, 2024. https://doi.org/10.1038/s41598-024-51578-7

[202] M. Aurangzeb, Y. Wang, S. Iqbal, A. Naveed, Z. Ahmed, M. Alenezi, and M. Shouran, "Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 51, No. 2, 2025, pp. 156-223
DOI: https://doi.org/10.25195/ijci.v51i2.637
Print ISSN: 2313-190X, Online ISSN: 2520-4912

blockchain privacy-preserving storage," *Energy Reports*, vol. 11, pp. 2493-2515, 2024. https://doi.org/10.1016/j.egyr.2024.02.010

[203] A. Bondok, M. Badr, M. Mahmoud, M. Alsabaan, M. Fouda, and M. Abdullah, "Securing One-Class Federated Learning Classifiers Against Trojan Attacks in Smart Grid," *IEEE Internet of Things Journal*, vol. 12, pp. 4006-4021, 2025. https://doi.org/10.1109/JIOT.2024.3481213

[204] D. Javeed, M. Saeed, I. Ahmad, M. Adil, P. Kumar, and A. Islam, "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," *Future Generation Computer Systems*, vol. 160, pp. 577-597, 2024. https://doi.org/10.1016/j.future.2024.06.023

[205] M. Singh, H. Singh, and A. Pratap, "Energy-Efficient and Privacy-Preserving Blockchain Based Federated Learning for Smart Healthcare System," *IEEE Transactions on Services Computing*, vol. 17, pp. 2392-2403, 2024. https://doi.org/10.1109/TSC.2023.3332955

[206] H. A. Al-Tameemi, G. G. Shayea, M. Al-Zubaidie, Y. L. Khaleel, M. A. Habeeb, N. A-H. K. Hussein, R. Z. Homod, M. Aljanabi, O.S Albahri, A. H. Alamoodi, M. M. Mijwil, M. A. Fadhel, I. M. Sharaf, M. G. Yaseen, A. H. Ali, U. S. Mahmoud, S. M. Mohammed, and A. S. Albahri, "A Systematic Review of Metaverse Cybersecurity: Frameworks, Challenges, and Strategic Approaches in a Quantum-Driven Era," *Mesopotamian Journal of CyberSecurity*, vol.5, no.2, pp.770–803, July 2025. https://doi.org/10.58496/MJCS/2025/045

[207] H. Zhang, S. Jiang, and S. Xuan, "Decentralized federated learning based on blockchain: concepts, framework, and challenges," *Computer Communications*, vol. 216, pp. 140-150, 2024. https://doi.org/10.1016/j.comcom.2023.12.042

[208] R. Mandava, "Assessing Creativity in Text-to-Image Generation: A Quantitative Analysis using Structured Human Rating Metrics," *International Journal of Innovative Technology and Interdisciplinary Sciences*, vol.8, no.2, pp.355–373, 2025. https://doi.org/10.15157/IJITIS.2025.8.2.355-373

[209] A. H. Elias, F. A. Khairi, and A. H. Elias, "Hybrid Machine-Learning Framework for Predicting Student Placement," *Journal of Transactions in Systems Engineering*, vol.3, no.2, pp.403–419, 2025. https://doi.org/10.15157/JTSE.2025.3.2.403-419

[210] T. MZILI, M. Mzili, S. I. Bouderba, A. Abatal, W. Aribowo, and A. K. Arya, "Interoperability in Internet of Things: Taxonomies and Open Challenges," *Babylonian Journal of Internet of Things*, vol.2025, pp.101-112, 2025. https://doi.org/10.58496/BJIoT/2025/005