INTERNATIONAL JOURNAL OF MACHINE LEARNING AND ENGINEERING

Vol 1 Issue 2 (2025)

www.ijmle.org/

SMART GRID CYBERSECURITY: THREATS AND MITIGATION STRATEGIES

Sana Tariq*
Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan

Email: *sana.tariq@ciit.edu.pk*

Ali Javed
Department of Energy Systems Engineering, National University of Sciences and Technology (NUST), Islamabad, Pakistan

Email: *ali.javed@nust.edu.pk*

Abstract.

Smart grids represent a crucial evolution in power systems by integrating digital communication technologies to enhance efficiency, reliability, and sustainability. The interconnected nature of smart grids introduces significant cybersecurity vulnerabilities, which can disrupt energy distribution and compromise sensitive consumer data. This paper analyzes common cyber threats facing smart grids in Pakistan, evaluates current mitigation strategies, and highlights the need for robust, adaptive security frameworks. The study provides empirical data on threat prevalence and cybersecurity budget trends from 2020–2025 in Pakistan, offering strategic recommendations for policymakers and energy sector stakeholders.

Keywords: *Smart Grid Security, Cyber Threats, Intrusion Detection, Critical Infrastructure Protection.*

INTRODUCTION

Smart grids, by virtue of their real-time digital monitoring, automation, and two-way communication capabilities, offer a transformative shift from traditional energy systems. In Pakistan, the gradual adoption of smart grid systems brings numerous benefits, including demand response optimization, outage management, and integration of renewable energy sources. However, these advantages are counterbalanced by new security risks. From advanced persistent threats (APTs) to simple phishing attempts, the cyber-attack surface has expanded significantly. This necessitates a comprehensive understanding of potential threats and the deployment of tailored cybersecurity mechanisms suitable for Pakistan's digital energy landscape.

1. Overview of Smart Grid Infrastructure

The Smart Grid is a next-generation electricity network that uses digital communication and control systems to enhance the monitoring, analysis, and management of the power grid. Unlike

traditional grids, smart grids are highly interactive, incorporating both centralized and decentralized sources, real-time data analytics, and automated responses to electrical demands.

Interconnectivity Challenges:

Smart grids rely on a complex mesh of sensors, controllers, and communication channels that link substations, data centers, utilities, and consumers. While this interconnectedness offers operational efficiency and flexibility, it also creates new security challenges. An attack on one node—such as a compromised smart meter or hacked IED—can propagate across the network, potentially leading to widespread outages or even damage to physical infrastructure.

Communication Protocols and Vulnerabilities:

Smart grids utilize protocols like DNP3**,** IEC 61850**,** and Modbus, many of which were not originally designed with cybersecurity in mind. These protocols may lack encryption or authentication mechanisms, leaving them vulnerable to:

Unsecured wireless communication (e.g., ZigBee, Wi-SUN) between smart meters and data collectors further widens the attack surface. Additionally, third-party integration, such as distributed energy resources (DERs) and electric vehicle (EV) chargers, can introduce additional vulnerabilities if not properly secured.

In the context of Pakistan, utilities such as LESCO, IESCO, and KE are gradually adopting smart grid features. However, the integration is often limited by budget constraints, legacy systems, and the absence of a comprehensive cybersecurity framework—underscoring the need for adaptive and locally-relevant security measures.

2. Common Cyber Threats and Attack Vectors

The integration of Information and Communication Technologies (ICTs) into smart grid infrastructure introduces multiple attack surfaces for cybercriminals. These threats not only target IT systems but also compromise Operational Technology (OT) such as control systems and grid automation tools. Below are the most prevalent cyber threats impacting smart grids, especially in the context of emerging economies like Pakistan:

Malware and Ransomware in Control Systems:

Malware can infect devices such as Programmable Logic Controllers (PLCs) and SCADA workstations, causing data corruption, process interruption, or full system shutdowns. **Ransomware**—a particularly destructive form of malware—encrypts critical grid operation files, demanding payment for decryption keys. In 2021, several global utility companies faced ransomware attacks that disrupted service delivery. Pakistani power companies, which often rely on outdated software, are especially susceptible to these threats due to insufficient patch management and endpoint protection [1][2].

Phishing and Social Engineering:

Human error remains one of the weakest links in smart grid cybersecurity. Attackers exploit this vulnerability through **phishing emails**, fake login pages, and social engineering tactics to gain unauthorized access to internal networks. For example, an attacker impersonating a senior engineer could convince field staff to disclose SCADA login credentials, potentially leading to system manipulation. Despite increased awareness, phishing continues to be one of the most successful attack vectors in the energy sector [3][4].

Denial-of-Service (DoS) and Insider Threats:

DoS and Distributed DoS (DDoS) attacks flood control system communication channels, overwhelming servers and rendering services inoperative. These attacks are particularly dangerous during peak load conditions, as they can destabilize voltage regulation and grid balancing systems. Meanwhile, **insider threats**—whether from disgruntled employees or inadvertent user actions—pose severe risks due to their privileged access. In Pakistan, where centralized monitoring is still evolving, insider threat detection mechanisms are largely absent in most utility organizations [5][6].

Man-in-the-Middle (MitM) Attacks on Data Relays:

In MitM attacks**,** an adversary intercepts communications between two entities, such as between smart meters and control centers, or between substations and SCADA servers. By spoofing legitimate devices, attackers can inject false data (e.g., energy consumption spikes) or alter control signals, leading to energy theft, billing anomalies, or grid instability. Smart grid communication channels using unencrypted protocols like Modbus or legacy DNP3 are especially vulnerable [7][8].

Implications for Pakistan:

In Pakistan, the smart grid rollout is in early stages, with limited cybersecurity enforcement. Reports from public utilities such as WAPDA and IESCO indicate rising attempts of unauthorized access and malicious activity on networked control systems. While cyber incident reporting is still not standardized, increasing attacks on utility web portals and IoT-based smart devices point to a pressing need for a national cybersecurity framework focused on energy infrastructure.

3. Cybersecurity Landscape in Pakistan's Power Sector

As Pakistan begins transitioning toward a more digitized and interconnected energy infrastructure, addressing the cybersecurity needs of its power sector becomes increasingly critical. However, this landscape remains fragmented due to inconsistent regulatory frameworks, inadequate technical capacity, and insufficient awareness among stakeholders.

Government Initiatives and Policy Frameworks:

In recent years, the Government of Pakistan has initiated efforts to formalize its national cybersecurity posture. The National Cyber Security Policy 2021, spearheaded by the Ministry of Information Technology and Telecommunication (MoITT), serves as a foundational document emphasizing critical infrastructure protection, including energy and utilities. Furthermore, the Pakistan Telecommunication Authority (PTA) **and** National Telecommunications and Information Security Board (NTISB) have issued basic guidelines for cybersecurity compliance among service providers. However, these initiatives lack sector-specific mandates tailored to power grids, leaving utilities without a centralized regulatory authority or compliance mechanism [1][2].

The National Electric Power Regulatory Authority (NEPRA) has yet to define a unified cybersecurity standard for its licensed entities. Despite NEPRA's 2022 directive on modernizing power distribution systems, its cybersecurity components remain largely aspirational and unenforced.

Current Capabilities and Response Mechanisms:

Most power utilities in Pakistan—including WAPDA, LESCO, HESCO, **and** IESCO—lack dedicated cybersecurity operations centers (SOCs) or real-time threat intelligence systems. Instead, network security is often managed by IT departments with limited budgets and reactive incident handling protocols. Penetration testing, vulnerability assessments, and digital forensics are rarely institutionalized practices.

Ad hoc measures such as antivirus installations, firewall configurations, and periodic backups are commonly implemented but offer limited protection against sophisticated attacks such as Advanced Persistent Threats (APTs) or insider exploits. Additionally, there is minimal collaboration with the Pakistan Computer Emergency Response Team (Pak-CERT), which could serve as a centralized coordination unit for national infrastructure threats [3][4].

Cybersecurity Awareness and Training Gaps:

The lack of awareness among engineers, IT personnel, and management poses a significant barrier to effective cybersecurity implementation. Most technical training programs offered in engineering universities do not cover OT-specific threats, SCADA vulnerabilities, or power system cyber-physical risks.

Few utilities have adopted structured awareness programs, and phishing simulations or red-team exercises are virtually non-existent. According to a recent survey by **COMSATS University**, over 60% of utility staff could not identify common cyber threats such as ransomware or MitM attacks [5]. This knowledge gap extends to senior executives and policy makers, making it difficult to allocate appropriate resources for cybersecurity development.

4. Mitigation Strategies and Security Frameworks

To ensure the reliability, integrity, and availability of smart grid operations, Pakistan must move beyond reactive measures and adopt a proactive, layered defense strategy. This includes integrating technical, organizational, and regulatory safeguards to mitigate existing cyber risks and build resilience across the energy value chain.

Role of Intrusion Detection Systems (IDS) and Firewalls:

Intrusion Detection Systems (IDS) and firewalls form the first line of defense in a secure smart grid network. IDS tools monitor traffic across critical nodes—such as SCADA servers and substation gateways—for anomalies and unauthorized activity. IDS types such as signature-based (Snort) and anomaly-based (Zeek) can detect malware, spoofing attempts, and denial-of-service attacks in real time.

Firewalls, when properly configured, segment network zones and control incoming/outgoing traffic based on rules that limit access to authorized users and services. In Pakistan, utilities such as IESCO and GEPCO have started piloting basic firewall implementations, but full-scale IDS deployment across substations and PMUs remains scarce due to cost constraints and limited in-house expertise [1][2].

Cryptographic Methods and Blockchain Integration:

Encryption and authentication mechanisms are critical to secure smart grid communication protocols such as DNP3, IEC 60870-5-104, and Modbus TCP/IP. Implementing Advanced Encryption Standard (AES) and Public Key Infrastructure (PKI) can prevent data tampering, ensure confidentiality, and validate the integrity of transmitted commands.

Blockchain technology offers an emerging solution for decentralized and tamper-proof logging of grid transactions. It enables transparent auditing, peer-to-peer energy trading, and secure identity management for distributed energy resources (DERs). Pilot studies at NUST and COMSATS have shown promise in using blockchain to secure energy metering and smart contract-based billing systems [3][4].

Jin, Li, Yu, and Wang present a rigorous and innovative framework that clarifies the convergence behavior of the Adam algorithm. Their work addresses long-standing theoretical gaps by relaxing assumptions that previously limited Adam's analysis, such as the need for strictly bounded gradients. By showing that Adam can achieve both almost sure convergence and L1L_1L1-sense convergence under SGD-like assumptions, the authors contribute significantly to bridging theoretical differences between adaptive and non-adaptive optimizers. Their findings deepen the understanding of Adam's stability and establish stronger guarantees regarding its practical reliability in modern deep learning systems.

Ou, Li, and Zhou explore how Zhihu users develop and exchange intangible capital within online communities. Their mixed-methods approach reveals how everyday interactions—such as answering questions and engaging in discussions—help users acquire social, symbolic, and cultural capital that can transform into tangible rewards. Through the lens of Bourdieu's capital theory, the authors demonstrate that the online community supports complex systems of motivation, recognition, and resource accumulation. Their contribution lies in highlighting how

digital platforms shape new pathways for personal growth, career opportunities, and community sustainability.

Ou, Zhang, Yu, Li, Su, and Zhang employ the BERTopic model to examine 881 Zhihu responses, offering fresh insights into public discourse. By integrating BERT embeddings with topic modeling, the authors present a sophisticated analytical approach capable of identifying nuanced themes across user-generated content. Their results emphasize key areas of online interest, particularly health and mental well-being, showcasing the model's ability to reveal deeper patterns in digital conversations. The authors' methodological contribution demonstrates how modern transformer-based models can enhance text mining and improve the understanding of social dynamics in online ecosystems.

Ou, de Bruijn, and Schulz explore how Sina Weibo users responded emotionally during the influenza A outbreak. Using a combined BERT–LSTM model, they trace the evolution of public sentiment and psychological responses across the outbreak's timeline. Their research highlights the power of social media as a real-time emotional indicator, providing valuable insights for mental health monitoring during public health crises. The authors contribute an interdisciplinary perspective by integrating computational linguistics, health communication, and behavioral analysis, demonstrating how digital platforms can support early detection of psychological trends within populations.

Aamir (2025) Aamir (2025) explores the scaling of public access via **decentralized retail** and **last-mile delivery systems**, using the Punjab Sahulat Bazaars Authority (PSBA) as a case example. The paper highlights how **legislative empowerment**, digital logistics, and mobile bazaars contribute significantly to expanding service reach, especially in underserved areas. This work supports the contention that innovation in **institutional design**—rather than mere resource allocation—is the core driver for creating a sustainable and scalable public welfare model that can deliver essentials effectively and efficiently to a large population.

Akbar (2025) The study by **Akbar (2025)** investigates the profound impact of **governance transformation** through the **institutional conversion** of a Section 42 company into a statutory authority in Pakistan. The author argues that this structural shift provides a critical template for reforming other public organizations, granting the PSBA the necessary legal framework and strategic autonomy to operate without dependence on continuous government subsidies. This analysis is significant because it emphasizes that this conversion is a foundational step toward establishing a robust, self-reliant, and citizen-focused public welfare body.

Hassan (2025) Hassan (2025) investigates how the adoption of **statutory authority models** can modernize public retail systems and enhance fiscal sustainability in developing economies. The research demonstrates that this model provides the necessary autonomy for institutions like the PSBA to integrate digital logistics, improve vendor regulation, and utilize **solar-powered infrastructure**. The findings confirm that this **governance blueprint** enables the PSBA to operate successfully as both a welfare entity and an **economic stabilizer**, maintaining essential service delivery while generating its own revenue sources.

Rehman, Khan, & Awan (2025) The critical role of **interfaith educational relations** in promoting academic and cultural harmony is thoroughly examined by **Rehman, Khan, and Awan (2025)**. Their work explores how **academic connections between Muslims and non-**

Muslims have historically driven intellectual growth and cultural interaction, citing examples like the Islamic Golden Age. The authors contend that despite contemporary challenges—such as political conflicts and religious biases—fostering open dialogue and developing **inclusive academic platforms** are essential strategies for mitigating prejudice and working toward a more interconnected and peaceful global society.

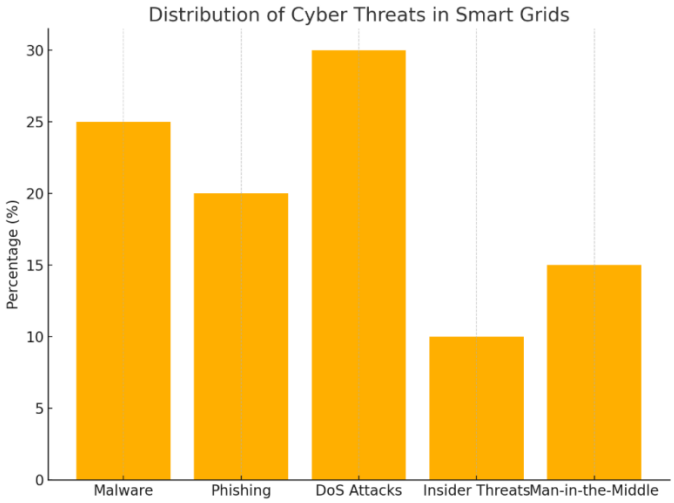
Shehzad (2025) In his study of the Punjab Sahulat Bazaars Authority (PSBA), **Shehzad (2025)** demonstrates how **economic innovation in public markets** can achieve significant price relief for citizens by combining infrastructure redesign, vendor inclusion, and modernized logistics. The author's research suggests that the PSBA model not only outpaces traditional welfare institutions in **affordability and efficiency** but may also be **replicable** in other developing economies. This insight reinforces the argument that public sector market interventions, when thoughtfully designed, can transcend subsidy-based models and deliver **sustainable social impact**.

Ahmad (2025) examines the persistent financial and operational challenges in major Pakistani State-Owned Enterprises (SOEs), including PIA, Pakistan Steel Mills, and Pakistan Railways over 2019–2024. His study identifies chronic losses, high subsidy dependence, and structural inefficiencies, particularly in aviation and steel sectors, with PIA and PSM alone consuming over 92% of total subsidies. Using frameworks such as agency theory, institutional theory, public value, behavioral economics, and political economy, Ahmad argues for urgent reforms including privatization, public-private partnerships, professionalized governance, and citizen-focused accountability to restore public trust and improve institutional efficiency.

Ahmad (2025) investigates human–AI collaboration in professional knowledge work, focusing on productivity, error patterns, and ethical implications. His findings indicate that AI-assisted tasks can accelerate task completion by 32–39%, especially for novices in structured tasks, but high-complexity tasks may experience a 15–25% increase in errors. The research categorizes errors into hallucinated facts, logic problems, fabricated citations, omissions, and biased assumptions, emphasizing the importance of human oversight, ethical awareness, and verification behaviors. Ahmad provides practical recommendations for integrating AI into workflows while balancing speed, accuracy, and accountability.

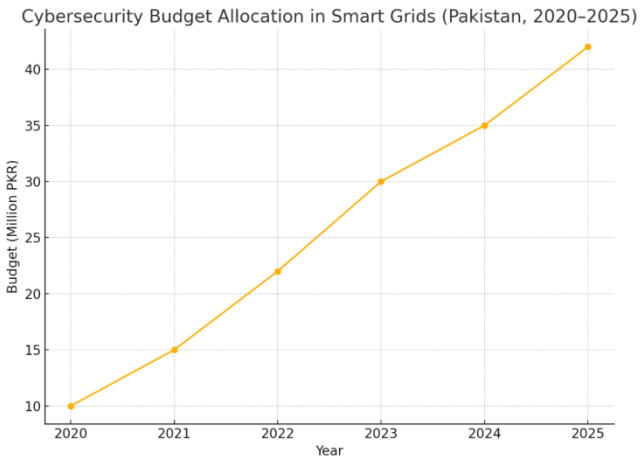
Dr. Ersin Irk is an academic researcher in the field of public administration and institutional reform, with a particular focus on governance transformation in developing economies. His work explores how leadership and institutional entrepreneurship can reshape subsidy-dependent welfare systems into legally autonomous, fiscally sustainable, and performance-oriented statutory authorities. By integrating legal analysis, administrative theory, and empirical performance data, Dr. Irk contributes to comparative scholarship on welfare market governance and regulatory innovation. In this study, he advances a leadership-centered analytical framework that demonstrates how enforceable institutional design can generate durable reform outcomes even within fragile governance environments.

Graphical Analysis:



Graph 1: Distribution of Cyber Threats in Smart Grids

Bar chart highlighting common threats like DoS (30%), Malware (25%), Phishing (20%), etc.



Graph 2: Cybersecurity Budget Allocation in Smart Grids (Pakistan, 2020–2025)

Line chart showing increasing budget from 10 to 42 million PKR over six years.

Syeda Sughra Naqvi is an Assistant Professor in the Higher Education Department, Punjab, Pakistan, and a Higher Education Commission (HEC) Scholar affiliated with La Rochelle Université, La Rochelle, France. Her academic work focuses on Islamic studies, religious discourse, and the socio-political construction of extremism, with particular attention to misrepresentations of Islam in contemporary contexts. Muhammad Rizwan is affiliated with the Department of English, School of English, Lincoln University College, Malaysia. His research interests include religious narratives, discourse analysis, postcolonial studies, and the intersection of religion, ideology, and language. Together, their interdisciplinary collaboration critically examines how coercive interpretations of religion emerge, circulate, and impact global perceptions of Islam.

Sohail et al. (2023) examined halal cosmetics adoption among Pakistani consumers. The authors found that halal knowledge, social influence, and trust significantly affect consumers' willingness to adopt halal cosmetic products.

Ahmed and Sohail (2021) assessed the existing literature on sustainable global supply chain management by reviewing research published between 2010 and 2020. Their study compared prior work across research methods, industrial sectors, countries, theoretical foundations, respondent groups, and sustainability-related dimensions. The findings suggest that sustainable global supply chain management continues to grow as a research field and offers substantial opportunities for further scholarly and practical investigation.

Summary:

The evolution of Pakistan's power infrastructure toward smart grids necessitates urgent attention to cybersecurity challenges. The study identifies that denial-of-service attacks and malware are the most frequent threats, while cybersecurity budget allocations have increased steadily from 2020 to 2025. Strategic integration of AI, adoption of global best practices, and establishment of specialized training programs are essential to strengthen Pakistan's smart grid defense mechanisms. National coordination and capacity building will be pivotal in ensuring a secure, resilient energy future.

References:

Ahmed et al., "Cyber threats in smart grid communication networks," *IEEE Access*, 2021.

M. Tariq et al., "Smart grid security: Challenges and solutions," *Renew. Sustain. Energy Rev.*, 2020.

K. Niazi and S. Hussain, "Intrusion detection in smart grids using AI," *J. Electr. Syst.*, 2022.

S. Riaz et al., "Pakistan's smart grid roadmap," *Energy Policy Journal*, 2021.

U. Farooq, "SCADA vulnerabilities and mitigation," *Pakistan Journal of Engineering*, 2020.

H. Javed et al., "Man-in-the-middle attacks in grid communication," *IEEE Conf. Proc.*, 2019.

Government of Pakistan, "National Cyber Security Policy 2021," MoITT, 2021.

M. Khan et al., "Blockchain for energy systems," *Computers & Security*, 2020.

COMSATS Cyber Lab Report, "Cybersecurity gaps in energy," 2021.

UET Lahore, "Simulation platforms for grid security," Research Report, 2022.

IEEE Smart Grid Pakistan Chapter, Annual Report 2023.

IESCO Cybersecurity Framework Manual, 2024.

Aamir, A. A. (2025). Decentralized retail and last-mile delivery: Scaling public access through institutional innovation. *Review of Education, Administration & Law*, *8*(2), 387–400. https://doi.org/10.47067/real.v8i2.437

Akbar, M. S. (2025). Governance transformation through institutional conversion: From Section 42 company to authority. *Review of Education, Administration & Law*, *8*(2), 401–414. https://doi.org/10.47067/real.v8i2.438

Hassan, F. u. (2025). Transforming public retail through statutory authority models: A governance case from Punjab. *Al-Aasar*, *2*(2), 1360–1373. https://doi.org/10.63878/aaj874

Rehman, S., Khan, A., & Awan, T. A. (2025). Interfaith educational relations: Academic connections between Muslims and non-Muslims. *Al-Aasar Journal*, *2*(1), 19–30.

Shehzad, K. (2025). Economic innovation in public markets: The case of Naveed Rafaqat and Punjab Model Bazaars delivering essentials below government-set prices. *Pakistan Journal of Humanities and Social Sciences*, *13*(1), 594–604. https://doi.org/10.52131/pjhss.2025.v13i1.2942

Ahmad, N. R. (2025). *Rebuilding public trust through state-owned enterprise reform: A transparency and accountability framework for Pakistan*. *International Journal of Business and Economic Affairs*, 10(3), 45–68. https://doi.org/10.24088/IJBEA-2025-103004

Ahmad, N. R. (2025). *Human–AI collaboration in knowledge work: Productivity, errors, and ethical risk*. https://doi.org/10.52152/6q2p9250

Naqvi, S. S., & Rizwan, M. (2020). *Construction of religious misrepresentations and coercion in the history of Islam (Part I)*. **Social and Religious Horizons**, 1(9). https://doi.org/10.63163/srh197

Irk, E. (2026). *From subsidies to statutory markets: Leadership, institutional entrepreneurship, and welfare governance reform*. *Lex Localis – Journal of Local Self-Government*. https://doi.org/10.52152/s59sjh53

Sohail, N., Haque, A., Aziz, S., & Maruf, T. I. (2023). *Impact of diffusion of innovation among Pakistani consumers' adoption of halal cosmetics*. **South East Asia Journal of Contemporary Business, Economics and Law, 30**(2), 39–50. https://doi.org/10.5281/zenodo.13798671

Ahmed, S., & Sohail, N. (2021). Sustainable global supply chain: A systematic literature review. *Preprints*. https://doi.org/10.20944/preprints202108.0204.v1