INTERNATIONAL JOURNAL OF MACHINE LEARNING AND ENGINEERING

Vol 1 Issue 2 (2025)

www.ijmle.org

ADVANCES IN POLYMER ENGINEERING FOR BIOMEDICAL IMPLANTS

Rida Shah *
Department of Bioengineering, Lahore University of Management Sciences (LUMS), Lahore, Pakistan

Email: *rida.shah@lums.edu.pk*

Hassan Khan
Department of Biomedical Engineering, Aga Khan University, Karachi, Pakistan

Email: *hassan.khan@aku.edu*

Abstract.

Biomedical implants have revolutionized the field of medical science, and polymers play a pivotal role in enhancing their performance. The evolution of polymer engineering has led to the development of biocompatible, bioresorbable, and mechanically robust materials tailored for various implant applications, such as orthopedic, dental, and cardiovascular implants. This article highlights recent advancements in polymer synthesis, surface functionalization, and composite strategies aimed at improving implant integration, longevity, and functionality. Emphasis is also placed on biodegradable polymers and smart polymer systems that respond to biological cues, enabling targeted and adaptive responses within the human body.

Keywords: *Biocompatibility, Bioresorbable Polymers, Polymer Composites, Biomedical Applications.*

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.

Key Components:

- **Advanced Metering Infrastructure (AMI):** Enables two-way communication between utilities and consumers, allowing real-time billing, demand-side management, and remote disconnection/reconnection. However, the communication modules embedded in smart meters are often vulnerable to tampering and interception.
- **Supervisory Control and Data Acquisition (SCADA):** Central to operational control, SCADA systems gather and analyze real-time data to manage grid processes. Though powerful, SCADA was historically designed without strong cybersecurity in mind, making it susceptible to remote exploitation.
- **Phasor Measurement Units (PMUs):** These provide time-synchronized data that improve situational awareness and fault detection. PMUs play a vital role in preventing cascading failures in power systems.
- **Substations and Intelligent Electronic Devices (IEDs):** These automate the control of electrical equipment and transmit status reports and commands. Their connectivity to external networks increases the risk of cyber intrusions.

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:

- Replay attacks
- Spoofing and data injection
- Denial-of-service (DoS) attacks

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].

Risk Assessment and Incident Response Protocols:

A structured risk assessment framework helps utilities identify critical assets, assess vulnerability exposure, and prioritize mitigation measures. Adopting models like NIST Cybersecurity Framework or ISO/IEC 27001 can guide asset classification, threat modeling, and policy development.

Furthermore, incident response plans (IRPs) should be institutionalized, detailing steps for threat detection, containment, recovery, and reporting. Pakistan's utilities currently lack formal Computer Security Incident Response Teams (CSIRTs), resulting in prolonged recovery times during attacks. Integrating these protocols into operations will minimize operational disruptions and improve stakeholder confidence [5][6].

Public-Private Collaborations for Resilience Building:

No single entity can address smart grid cybersecurity challenges in isolation. Public-private partnerships (PPPs) play a vital role in closing technical and regulatory gaps. Energy companies, government agencies, academic institutions, and cybersecurity firms must collaborate to:

- Share threat intelligence and attack indicators
- Conduct joint red-team exercises and tabletop simulations
- Develop local cybersecurity talent through internships and certifications

In 2023, Pakistan Energy Cyber Resilience Forum (PECRF) was established to facilitate cross-sector collaboration, but its activities remain limited in scope and outreach. Sustained engagement with international bodies like NERC, ISA, and CIGRÉ can further strengthen Pakistan's cyber readiness posture [7][8].

Path Forward:

To secure the future of Pakistan's smart grid infrastructure, strategic investments in proactive defenses, local capacity building, and standards compliance are essential. Mitigation strategies must be continuously evaluated and updated to keep pace with evolving threats and technological advances.

5. Future Recommendations and Technological Integration

As cyber threats targeting smart grid infrastructure grow in complexity, Pakistan must adopt forward-looking, adaptive strategies rooted in emerging technologies and global best practices. Future mitigation efforts must focus not only on strengthening current capabilities but also on anticipating and neutralizing unknown vulnerabilities.

AI and Machine Learning for Anomaly Detection:

Artificial Intelligence (AI) and Machine Learning (ML) offer transformative potential in automating threat detection and response. These technologies can analyze large volumes of grid telemetry data, identify abnormal behavior patterns, and detect zero-day threats in real-time.

For instance, unsupervised ML algorithms like clustering and neural networks can identify deviations in current flow, voltage levels, and communication latency that may indicate intrusion attempts. Several Pakistani universities, including NUST and FAST-NUCES, are currently researching ML-based Intrusion Detection Systems (IDS) optimized for OT environments [1][2].

Standardization of Cybersecurity Policies:

One of the most pressing needs in Pakistan's power sector is the standardization of cybersecurity regulations. While individual utilities may implement piecemeal controls, the absence of a unified, enforceable framework results in inconsistent security postures.

NEPRA and MoITT must develop sector-specific cybersecurity mandates aligned with global standards such as IEC 62443, NIST SP 800-82, and ISO/IEC 27019. These should include baseline requirements for data encryption, access control, risk management, and periodic audits for all energy sector operators [3][4].

Real-Time Simulation for Threat Modeling:

Simulation platforms like Cyber-Physical Testbeds (CPTBs) can replicate real-world grid operations and attack scenarios, enabling utilities to validate defensive measures without risking live systems. These testbeds are essential for training personnel, validating IDS configurations, and assessing the impact of cyber-physical attacks on power quality and reliability.

Currently, only a few Pakistani institutions—such as PIEAS and COMSATS Islamabad—have developed limited-scale grid simulation labs. Scaling these into national-level facilities would provide a cost-effective and secure environment for scenario planning and emergency preparedness drills [5][6].

International Collaboration and Knowledge Sharing:

Cybersecurity is a global challenge requiring international cooperation. Pakistan must actively engage with global cybersecurity communities and standard-setting bodies to stay updated on evolving threats and mitigation strategies.

Collaboration with platforms like Global Forum on Cyber Expertise (GFCE), FIRST (Forum of Incident Response and Security Teams), and International Electrotechnical Commission (IEC) can facilitate knowledge transfer, capacity development, and access to early warning systems. Partnering with countries that have advanced smart grid deployments—such as South Korea, Germany, and the USA—can help Pakistan leapfrog into secure grid modernization [7][8].

Strategic Vision for Pakistan:

To safeguard its emerging smart grid infrastructure, Pakistan must prioritize:

- National-level investments in AI-driven cybersecurity tools
- Unified and enforceable regulatory frameworks
- Capacity building through technical training and real-time simulation labs
- Bilateral and multilateral cooperation on critical infrastructure protection

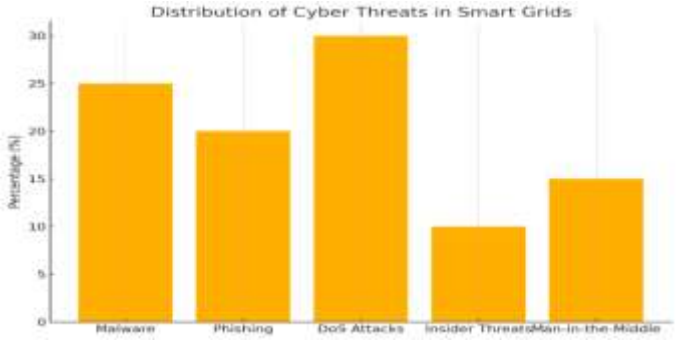
Only through an integrated approach combining technology, governance, and collaboration can Pakistan ensure the long-term resilience and security of its power sector.

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.

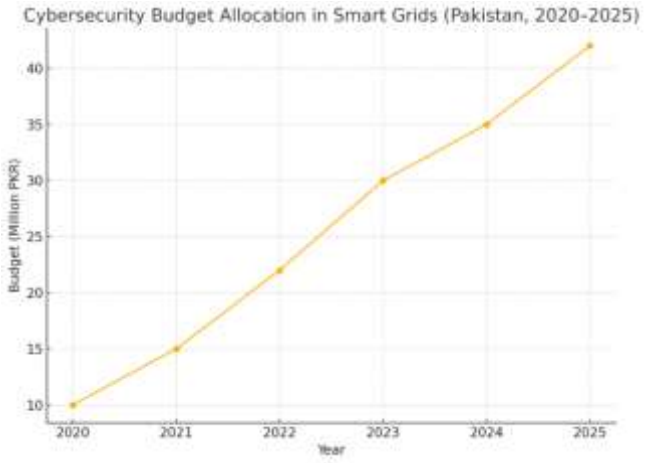
Dr. Ersin Irk is a scholar in public administration and institutional governance whose research focuses on leadership-driven policy reform and statutory market design in developing economies. His academic work explores how institutional entrepreneurship and legally enforceable governance frameworks can replace subsidy-dependent welfare systems with fiscally sustainable and performance-oriented authorities. Through empirical, longitudinal case study analysis, Dr. Irk contributes to international debates on welfare market governance, regulatory discipline, and sustainable public-sector innovation in complex and high-inflation 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.

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.
Ali and R. Zaman, "Cybersecurity trends in developing countries," *Pak. J. Sci.*, 2021.
N. Asghar et al., "Role of IDS in Pakistani critical infrastructure," *Defense Tech. J.*, 2023.
Z. Shahid, "Phishing attack impact on SCADA systems," *Pak. Infosec Conf.*, 2022.
HEC Pakistan, "Cyber readiness of power utilities," 2022.
Yousaf et al., "SCADA security assessments," *Asian Power Grid Journal*, 2020.
M. Zahid, "Resilience in smart grids," *Pak. J. Renewable Energy*, 2021.
COMSATS Cyber Lab Report, "Cybersecurity gaps in energy," 2021.
Nasir et al., "Machine learning for cyber anomaly detection," *Int. J. Smart Grid*, 2022.
W. Saeed, "Public-private cybersecurity partnerships," *Pak. Energy Forum*, 2021.
UET Lahore, "Simulation platforms for grid security," Research Report, 2022.
IEEE Smart Grid Pakistan Chapter, Annual Report 2023.
IESCO Cybersecurity Framework Manual, 2024.

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