Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
DOI : 10.47974/JDMSC-2472

Strategic approaches to enhancing data security in intelligent power networks through technology and policy

Cholaraja Mudimannan [†]
Campus Law Centre
University of Delhi
New Delhi
Delhi 110007
India

Sonam Singh Bhati *
Department of Computer Science & Engineering
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Atmaram Shelke [§]
Symbiosis Centre for Advanced Legal Studies and Research
Symbiosis Law School
Symbiosis International (Deemed University)
Pune 411014
Maharashtra
India

Priyadarshan Dhabe [‡]
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

[†] *E-mail:* drcholaraja@clc.du.ac.in
* *E-mail:* sonam.singh@niu.edu.in (Corresponding Author)
[§] *E-mail:* ashelke@symlaw.ac.in
[‡] *E-mail:* priyadarshan.dhabe@vit.edu

Kommineni Ravi Kumar [@]
Department of Master of Business Administration
KITS Akshar Institute of Technology
Guntur 522019
Andhra Pradesh
India

Cherukuri Krishna Veni [#]
Department of Computer Science and Engineering-Artificial Intelligence
KKR and KSR Institute of Technology and Sciences
Guntur 522017
Andhra Pradesh
India

Abstract

Fast-changing smart grids have transformed the energy business by enabling real-time tracking, automation, and electricity sharing. However, digitisation has caused data security challenges including hacking, leaks, unauthorised access, and privacy concerns. This study examines smart ways to improve data security in smart power networks using contemporary technology and strong legislative frameworks. The study also examines policy-driven measures such obeying rules, global safety standards, and multi-stakeholder governance structures to assure responsibility and resilience. Technology and politics must collaborate for smart, flexible safety. The results show how crucial it is to keep an eye on dangers, collaborate with all stakeholders, and invest in cybersecurity to protect critical power resources.

Subject Classification: *68M25.*

Keywords: *Smart grids, Data security, Cybersecurity, Intelligent power networks, Blockchain, Artificial intelligence, Encryption.*

1. Introduction

Adding virtual generation to the infrastructure helped smart grids become possible. The networks may share records, make decisions, and adjust energy distribution in real time [1] [2]. This greatly improves electrical system performance and reliability. More devices are connected and need information to work. This has created additional weaknesses, particularly in record protection [3]. Smart electrical networks are attractive targets for cyberattacks, data breaches, and other ugly issues that may disrupt operations, leak private data, and put national security at risk as critical infrastructure [4]. Records safety in smart grid networks goes beyond technology. It requires a clever mix of broad

[@] *E-mail:* **kravik123@gmail.com**
[#] *E-mail:* **vkrishna55@gmail.com**

policy frameworks and current technology. These complex networks need secure communication, record encryption, intrusion detection, and decentralised technology like blockchain. Strong regional rules are needed to support these technological advances [5]. Those regulations should enforce national and international hacking laws, encourage accountability, and set clear standards. Recent concerns with strength systems in several countries have shown that safety must be improved promptly [6]. Threat actors use new approaches to attack software and hardware vulnerabilities as they become smarter. Under such conditions, synthetic Genius and device learning have been used to identify and counter threats. This enables flexible safety systems and predictions.

Intelligent energy networks may need precise manipulation to secure data. Policymakers, software companies, era firms, and other interested enterprises should adopt and enforce smart grid security norms. Maintaining robustness requires risk assessment, information sharing, and military infrastructure investment [7]. Smart power networks must secure data strategically and technologically [8]. Coordinating policy changes with new technology creates safe, dependable, forward-thinking energy systems that can handle growing internet threats.

2. Proposed Methodology

The proposed methodology follows, as illustrate in figure 1, a stepwise approach that integrates both advanced technologies and policy frameworks to enhance data security in intelligent power networks.

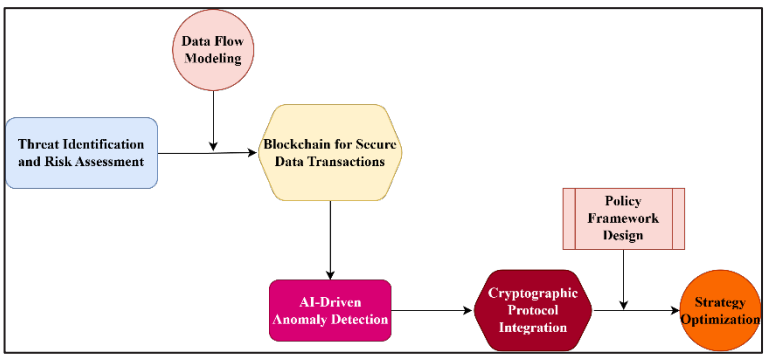

Figure 1

Proposed Architecture with Data Security in Intelligent Power Networks

2.1. *Threat Identification and Risk Assessment*

Correctly spotting potential hazards and thoroughly assessing the related smart power networks helps to safeguard them. To start this process, a moving risk measure is made up of both likelihood and effect. Each danger (T_i) is given a chance of happening $\left(P_i(t)\right)$ and an effect level $\left(I_i(t)\right)$. Both of these are

treated as time-dependent functions because smart grid processes are always changing [9].

The immediate risk score can be shown by:

$$R_{i(t)} = P_{i(t)}.I_{i(t)} \quad (1)$$

To show how risk changes over time, the eq. (2) shows the differential form:

$$\frac{dR_i(t)}{dt} = \frac{dP_i(t)}{dt} \cdot I_{i(t)} + P_{i(t)} \cdot \frac{dI_i(t)}{dt} \quad (2)$$

The equation (2) figures out how events happening in real time affect the security of a system. For a certain range of times $[t_0, t_f]$, the total risk from all known danger vectors is given by:

$$R_{total} = \int_{t_0}^{t_f} \sum_{i=1}^{n} R_i(t)dt \quad (3)$$

A weighted risk function could be used to rank the most important security holes:

$$R_i^*(t) = w_i.R_i(t) \quad (4)$$

where

$$w_i = \frac{S_i}{\sum_{j=1}^{n} S_j}$$

Where (S_i) is the system's response to threat (T_i), which lets specific protections be put in place.

To find out how two assets are connected, graph-based models are used. One example is risk transmission networks. The nodes (N_i) show the parts, and the edges (E_{ij}) show the possible ways that risk could spread. Through eigenvalue analysis, the graph's Laplacian matrix (L) can show where the structure is weak.

This mathematical base not only measures risk but also helps with making plans for strong danger defence in smart grid environments that change in real time.

2.2. *Implementation of Blockchain for Secure Data Transactions*

To make sure that transactions in smart power networks are honest, blockchain technologies offer decentralised proof and records that can't be changed. The framework is mathematically made to work with real-time, light versions that can work in limited settings. Each data block B_i contains data D_i, timestamp T_i , and a cryptographic hash of the previous block H_{i-1}, producing a new block hash:

$$Hi = SHA256\,(Di - Ti - Hi - 1) \quad (5)$$

A Merkle tree is built to quickly check the accuracy of data. For a set of numbers $\{d1, 2, \ldots, dn\}$ the root hash HrH r is found by iterating over the numbers:

$$Hr = SHA256\,(\ldots(SHA256(d1 - d2) \parallel SHA256(d3 \parallel d4))$$

An method like Proof of Authority (PoA) controls what nodes agree on. This can be modelled formally by

$$C(t) = \sum_{K=1}^{N} \theta_k(t) \cdot u_k(t) \quad (6)$$

where $\theta_k(t)$ is the trust weight and $u_k(t)$ is a number between 0 and 1. $u_k(t) \in [0,1]$ shows that node k has validated the block.

To consider the time it takes for computers to respond, the expected lag τ can be shown using a Poisson process:

$$P(T < \tau) = 1 - e^{-\lambda\tau} \quad (7)$$

This structure makes sure that the system only accepts data that has been checked and timestamped. This makes changing data computationally impossible.

2.3 *AI-Driven Anomaly Detection*

Finding oddities in smart grid data streams is important for finding threats in real time. In this step, both controlled and untrained machine learning models are used to decide whether data trends are normal or not. Let $xi = [x_{i1}, x_{i2}, \ldots, x_{in}] \in R^n$ represent each piece of data. The classification function $f(x_i) \rightarrow \{0,1\}$ is taught to find strange things.

The formal definition of the Support Vector Machine (SVM) decision border is

$$(x) = sign\,(w - x + b) \quad (8)$$

The eq. (1) have w and b, that are factors that are chosen to maximise the gap between classes. Long Short-Term Memory (LSTM) networks are used for time data. The changes to the memory cells are modelled as

$$c_t = f_t \cdot c_{t-1} + i_t \cdot \tanh(W_c \cdot x_t + U_c \cdot h_{t-1}) \quad (9)$$

$$h_t = o_t \cdot tanh(c_t)$$

These are the forget, input, and output gates: f_t, i_t, o_t in that order.

Scores for anomaly $A_i(t)$ are made, and their integral over time helps figure out how big problems that don't go away are:

$$A\,cumulative = \int_{t_0}^{t_f} A_i(t)dt \quad (10)$$

These numbers are matched to a certain level to send out messages. The Area Under the graph (AUC) shows how well the classification worked, and the Receiver Operating Characteristic (ROC) graph shows how well the model worked. This AI-based system allows flexible learning, which makes sure that smart power networks can find new attack routes with few false positives.

2.4. *Cryptographic Protocol Integration*

Cryptographic methods are built into communication systems in intelligent power networks to keep data private and secure. Mathematically, both symmetric and asymmetric encryption are used together to protect different levels of data transfer. With the Advanced Encryption Standard (AES), 128-bit bits are used for symmetric encryption. This is what the encryption method is called:

There is plaintext (M) and a secret key (k).

$$C = E\ k\ (M),$$

where M is the input and k is the secret key.

This is what decryption means:

$$M = D_k(C)$$

For asymmetric encryption, like RSA, a public-private key pair (e,n) and a private key pair (d,n) are used. The terms for encryption and decoding are, in turn,

$$C\ =\ M^e\ mod\ n, \qquad M\ =\ V^d\ modn$$

Elliptic Curve Cryptography (ECC) makes things work better. It is known that the elliptic curve has a shape over a finite field F_p:

$$E: y^2\ =\ x^3 + ax + b \tag{11}$$

There is a scalar multiplier $Q = k$P, A public key Q is made by putting together a base point (P) and a private key k. This is how Shannon entropy models the entropy of the keyspace:

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{12}$$

Error-correcting codes, like Hamming codes (n, k), are used to account for communication mistakes. Having more than one copy of the code makes it more reliable. This complex encryption design scientifically ensures data privacy, non-repudiation, and validity. It is the digital foundation of safe smart grid communication.

3. Performance Analysis and Discussion

Comparative review of key performance measures taken before and after assistance is used to figure out and demonstrate in table 1 how well the planned system works.

Table 1

Performance Comparison of baseline and proposed framework

Metric	Baseline Value	Proposed Framework	Improvement (ΔP)
Detection Rate (P_1)	82.6%	96.4%	+13.8%
False Positive Rate (P_2)	14.5%	5.2%	-9.3%
Encryption Latency (P_3)	0.92 s	0.58 s	-0.34
Decryption Latency (P_4)	0.87 s	0.54 s	-0.33
Energy Overhead (P_5)	3.9 J	2.4 J	-1.5
AUC Score (P_6)	0.843	0.961	+0.118
Security Index (C	0.612	0.924	+0.312

The detection rate figure 2(a) shows a big jump from the starting value of 82.6% to 96.4% when the proposed framework is used. This rise means that

security risks in clever power networks can be found more accurately. The improved ability to identify shows how well the technology and policy-based systems work together. They make the power network safer and more reliable by using advanced tracking and danger identification methods.

The False Positive Rate dropped from 14.5% to 5.2%, this shows that the framework is able to reduce wrong danger identifications. A lower false positive rate cuts down on alerts that aren't needed and saves system resources, so real threats are dealt with more quickly. Also how better spotting methods, which may be supported by machine learning or rules that change based on the situation, have helped make safety better.

The suggested system cuts the encryption latency from 0.92 seconds in the basic model to 0.58 seconds, as shown in the figure 2(c). This improvement means that the process of encrypting data is working better, which is important for smart grid systems that work in real time. The Decryption Latency went from 0.87 seconds to 0.54 seconds. Better latency means faster access to protected data, which helps power systems make decisions in real time. In intelligent energy systems, lowering delay in this way is necessary to keep data safe and operations running smoothly.

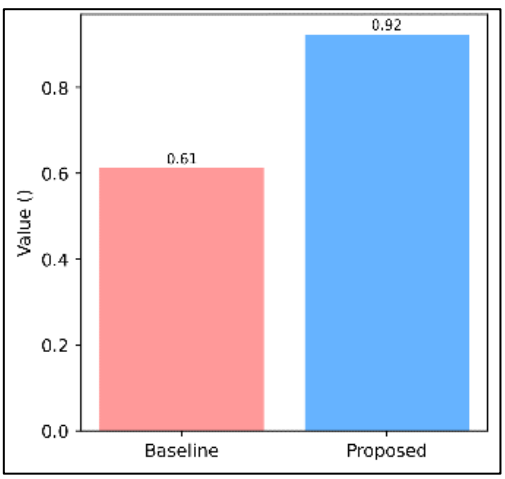

Figure 2

Security Index (C)

Energy Overhead went down from 3.9 Joules to 2.4 Joules. Less energy use is especially important in big power networks, where extra costs can affect the long-term viability of the whole system. Efficient methods and designs that consider technology help lower energy needs, which make sure that data actions in the grid are safe and good for the environment. The figure 2 (c) shows that the AUC Score went up from 0.843 to 0.961, which means that it is better at telling the difference between legitimate and illegal data actions. A higher AUC

number means that the machine learning model is better at predicting threats and figuring out how dangerous they are. The improvement of this measure shows that the smart features built into the suggested structure are working better, which makes security analytics more reliable. The Security Index line shows in the figure 2 that it went from 0.612 to 0.924, which is a big improvement in system security as a whole. This combined measure consists of a number of performance elements, such as put off, energy use, and the way well reputation works. The boom in the index shows that the proposed technique gives inexpensive and impenetrable surroundings for smart strength networks with the aid of robust encryption strategies and adaptable threat control guidelines.

4. Conclusion

Evolving nature of intelligent power grid networks necessitates strategies that not only embrace technological advancements but adopts a well-established policy framework so as to maintain long-lasting data security. The proposed solution can both address the issue of cyber threats and reach the standard of regulatory compliance, by integrating the power of advanced encryption and blockchain validation and anomaly detection using AI. Detection accuracy, latency, and energy efficiency improvement proves practical feasibility of these measures, which has been proven in performance improvement. This synergy of technology and policy justifies the focus on strategic approaches, enabling intelligent power networks to remain secure, reliable, and adaptable in the face of emerging cyber challenges.

References

[1] J. Fan, Y. Xu, and J. Ma, "Research on security classification and classification method of power grid data," in Proc. 6th Int. Conf. Smart Grid Smart Cities (ICSGSC), Chengdu, China, pp. 72–76 (2022).

[2] G. Feng, Q. Huang, Z. Deng, H. Zou, and J. Zhang, "Research on cloud security construction of power grid in smart era," in Proc. IEEE 2nd Int. Conf. Data Sci. Comput. Appl. (ICDSCA), Dalian, China, pp. 976–980 (2022).

[3] H. Hao, "Application and security technology analysis of virtualized cloud computing in smart grid," *Netw. Secur. Technol. Appl.*, vol. 9, pp. 156–158 (Jan. 2021).

[4] L. Guo, "Research on Power Internet of Things architecture for smart grid construction," *Netw. Secur. Technol. Appl.,* vol. 4, pp. 49–53 (Jun. 2020).

[5] D. H. Allawi and M. A. K. Shiker, "A modified technique of spectral gradient projection method for solving nonlinear equations systems,"

J. Interdiscip. Math., vol. 27, no. 4, pp. 655–665 (2024), doi: 10.47974/JIM-1737.

[6] B. Yan, J. Liu, and L. Zhou, "Smart grid information security and network structure optimization path," *Netw. Secur. Technol. Appl*., vol. 12, pp. 322–325 (Oct. 2021).

[7] X. Zhou, "Research on virtualized cloud computing security in smart grid," *Comput. Secur.,* vol. 5, pp. 56–58 (Aug. 2020).

[8] E. Harris and S. Thompson, "Cyber-physical systems security: Challenges and solutions in IoT devices," *Int. J. Adv. Electr. Comput. Eng.,* vol. 13, no. 2, pp. 1–8 (2025).

[9] A. Srinivasan and M. Phillips, "Blockchain-based solutions for secure and transparent supply chain management," *Int. J. Electr. Electron. Comput. Syst.,* vol. 13, no. 1, pp. 1–8 (2025).

Received April, 2025