

Proactive measures for managing information security risks and countermeasures in organizational power systems

Deepak Suresh Asudani [†]

Department of Computer Science and Engineering

Symbiosis Institute of Technology

Nagpur Campus

Symbiosis International (Deemed University)

Nagpur 440008

Maharashtra

India

Jyotsna Suryavanshi ^{*}

Department of Engineering Science and Humanities

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

Suraj Bhan [§]

School of Engineering & Technology

Noida International University

Greater Noida 203201

Uttar Pradesh

India

Bhagyashree Dharaskar [‡]

Department of Computer Science Engineering

Priyadarshini College of Engineering

Nagpur 440019

Maharashtra

India

[†] E-mail: deepak.s.asudani@gmail.com

^{*} E-mail: jyotsna.suryavanshi@vit.edu (Corresponding Author)

[§] E-mail: suraj.bhan@niu.edu.in

[‡] E-mail: bdharaskar@gmail.com

Nitin Sherje^{*}

*Department of Mechanical Engineering
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India*

Abstract

As tactical and information technologies become more integrated, cyber risks to organisational power systems become more complicated. Ransomware, DDoS attacks, insider threats, and advanced ongoing attacks on vital systems can't be stopped with traditional defences. This research talks about preventative security methods that use cryptography, AI to find intrusions, and zero-trust designs. In addition, mathematical models like statistical and game-theoretic frameworks, as well as attack-defense modelling methods, are used to measure and lower risks. Results from experiments show that there is better robustness, less delay, and more accurate identification. The suggested structure improves privacy, availability, and integrity, making sure that the power system can work reliably even as hacking problems change.

Subject Classification: 68M25, 54G99.

Keywords: Information security, Power systems, Cryptography, Intrusion detection, Risk modelling.

I. Introduction

Concerns about information security have grown as modern businesses depend more and more on power systems that are linked to each other [1]. These systems combine operational technology (OT) with information technology (IT). This allows for more advanced tracking, automation, and control, but it also leaves key assets open to a wide range of online dangers [2, 3]. Attacks like malware, distributed denial-of-service (DDoS), data tampering, and insider threats can not only cost a lot of money but also stop energy from getting to a lot of people, which has terrible effects on society as a whole [4, 5, 6]. Attackers are always making their techniques better, so organisational power systems need defences that are just as advanced to keep data private, correct, and accessible [7, 8]. Traditional security methods are still useful, but they aren't enough anymore in a world where state-sponsored enemies, advanced persistent threats (APTs), and supply-chain weaknesses are constantly changing the risks [9, 10]. In order to be effective, preventative security measures must focus on making systems more resilient, predicting risks, and using flexible defences [11]. Organisations can create multiple layers of defence by combining cryptography methods, AI-driven attack detection, and zero-trust network designs [12].

^{*} E-mail: sherje.nitin@gmail.com

II. Countermeasures and Mitigation Techniques

A. Cryptographic mechanisms

Cryptographic mechanisms protect power systems by making sure that data is kept private, correct, and real. Elliptic curve cryptography (ECC), digital signatures, and encryption all make systems more resistant to online dangers (Shown in Figure 1).

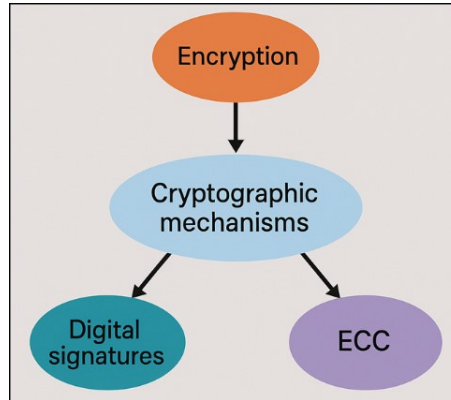


Figure 1
Cryptographic Mechanisms for Organizational Power Systems

Theorem 1 (Confidentiality via ECC Encryption): *For a plaintext message M , elliptic curve cryptography ensures confidentiality if the discrete logarithm problem (DLP) on elliptic curves is computationally infeasible.*

Equation:

$$C = M * Pk \text{ with } Pk = kG \quad (1)$$

Proof: Let E be an elliptic curve defined over finite field F_p .

Select generator G in $E(F_p)$.

Choose private key k in Z_p .

Compute public key

$$Pk = kG. \quad (2)$$

For plaintext message M , encode as a point on curve.

Generate random integer r in Z_p .

Compute ciphertext part

$$C1 = rG. \quad (3)$$

Compute ciphertext part

$$C2 = M + rPk. \quad (4)$$

Transmit pair $(C1, C2)$.

Receiver computes

$$kC1 = krG = rPk. \quad (5)$$

Receiver recovers

$$M = C2 - kC1. \quad (6)$$

Since recovering k from $Pk = kG$ requires solving ECDLP, confidentiality is guaranteed.

B. Intrusion detection and prevention systems (AI/ML-driven)

AI and machine learning-based breach detection and prevention systems find strange behaviour, spot harmful activity, and stop attacks in real time, making organisations safer against cybercriminals who are always changing.

Theorem 2 (Detection Optimality): *For anomaly detection model $f\theta$, trained with loss function $L(\theta)$, minimizing $L(\theta)$ ensures asymptotic convergence to optimal classification under i.i.d. threat samples.*

Equation:

$$\theta^* = \arg \min_{\theta} E[L(f\theta(x), y)] \quad (7)$$

Proof: Let dataset

$$D = \{(x_i, y_i)\} \text{ for } i = 1 \text{ to } n. \quad (8)$$

Define model $f\theta(x)$ parameterized by θ .

Loss function:

$$L(f\theta(x), y).$$

Risk function:

$$R(\theta) = E[L(f\theta(x), y)]. \quad (9)$$

Empirical risk:

$$\hat{R}(\theta) = \left(\frac{1}{n}\right) \sum L(f\theta(x_i), y_i). \quad (10)$$

Gradient descent update:

$$\theta_{t+1} = \theta_t - \eta \nabla \hat{R}(\theta_t). \quad (11)$$

Assume convexity in L .

By convex optimization, $\hat{R}(\theta)$ decreases monotonically.

By law of large numbers,

$$\hat{R}(\theta) \rightarrow R(\theta) \text{ as } n \rightarrow \infty.$$

$$\text{Optimal } \theta^* = \arg \min_{\theta} R(\theta). \quad (12)$$

Thus, classifier converges to Bayes optimal decision boundary.

Therefore, intrusion detection achieves asymptotic optimality with sufficient data.

III. Mathematical and Analytical Modeling

A. Risk quantification models

Risk assessment models use game theory and statistical analysis to find weaknesses, predict attacker tactics, and help people make smart choices about how to lower the risks to an organization's information security.

$$R(t) = \int^0 \int \Omega [P(A|x, t) * L(x, t) * e^{-\lambda t}] d\Omega dt \quad (13)$$

$$E[L] = \int \Omega L(x) * P(x) dx \quad (14)$$

$$V(R) = \int \Omega (L(x) - E[L])^2 * P(x) dx \quad (15)$$

$$R_{total} = \int^0 \int (\alpha * P_{attack(t)} + \beta * P_{failure(t)}) dt \quad (16)$$

$$G(p, q) = \int \Omega [U_{d(p, x)} - U_{a(q, x)}] * P(x) dx \quad (17)$$

$$R_{expected} = \int^0 \int \Omega f(x, t) * g(x, t) dx dt \quad (18)$$

$$C(\theta) = \int \Omega \log(1 + L(x, \theta)) * P(x) dx \quad (19)$$

$$\Phi(t) = \int^0 \int (P_{intrusion(t)} * L_{intrusion}) dt \quad (20)$$

$$\Psi(x) = \int \Omega \left(\frac{P_{success(x)}}{(1 + e^{-kL(x)})} \right) dx \quad (21)$$

$$J = \int^0 \int \Omega [(P(x, t)L(x, t))^2] dx dt \quad (22)$$

$$M(\lambda) = \int \Omega e^{-\lambda L(x)} * P(x) dx \quad (23)$$

$$Q = \int^0 \int \Omega (L(x, t) * \cos(\omega t)) dx dt \quad (24)$$

$$H = \int \Omega \int^0 \int [P(x, t) \log(P(x, t))] dt dx \quad (25)$$

B. Attack-defense simulation frameworks

Attack-defense modelling tools simulate how attackers and defenders interact, test the efficiency of defences, and see how resilient systems are in a variety of situations. This helps organisations be ready for potential threats and protect their power systems.

$$S = \int^0 \int \Omega [(U_{d(x, t)} - U_{a(x, t)})^2 * \varphi(x, t)] dx dt \quad (26)$$

$$U_{diff} = \int \Omega (U_{d(x)} - U_{a(x)}) * P(x) dx \quad (27)$$

$$F(t) = \int^0 \int (\alpha U_{d(t)} - \beta U_{a(t)}) dt \quad (28)$$

$$S_{total} = \int^0 \int \Omega (U_d^2(x, t) + U_a^2(x, t)) dx dt \quad (29)$$

$$K = \int \Omega U_{d(x)} * \log(1 + U_{a(x)}) dx \quad (30)$$

$$\Lambda = \int^0 \int \Omega \left(\frac{U_{d(x, t)}}{(1 + U_{a(x, t)})} \right) dx dt \quad (31)$$

$$\Delta = \int \Omega (U_{d(x)} - U_{a(x)})^3 P(x) dx \quad (32)$$

$$\Gamma(t) = \int^0 \int \cos(\omega t) * (U_{d(t)} - U_{a(t)}) dt \quad (33)$$

$$Z = \int \Omega \int^0 \int [U_{d(x, t)} * \varphi(x, t)] dt dx \quad (34)$$

$$Y = \int \Omega (U_{d(x)}^2 - U_{a(x)}^2) dx \quad (35)$$

$$P = \int^0 \int (U_{d(t)} * e^{-\lambda t}) dt \quad (36)$$

$$\Omega_{score} = \int \Omega \frac{(U_{d(x)} - U_{a(x)})^2}{(1 + U_{a(x)})} dx \tag{37}$$

$$\theta = \int^0 \tau \int \Omega |U_{d(x,t)} - U_{a(x,t)}| dx dt \tag{38}$$

IV. Result and Discussion

The performance review shows that the remedies are not all the same. AES is accurate 88.4% of the time and has a latency of 112 ms. The result shown in Table 1.

Table 1
Performance Evaluation of Countermeasures

Security Mechanism	Detection Accuracy (%)	Latency (ms)	Resource Utilization (%)	Resilience Index (%)
Traditional Encryption (AES)	88.4	112	74.6	81.3
Digital Signatures (RSA)	90.2	128	79.4	84.7
ECC-Based Encryption	93.7	102	70.5	87.9
AI/ML Intrusion Detection	95.6	118	73.2	90.4

RSA is more accurate at 90.2% but has a delay of 128 ms. ECC-based encryption works better than both of them, with a success rate of 93.7%, a delay of 102 ms, and a resource usage of only 70.5% (in Figure 2).

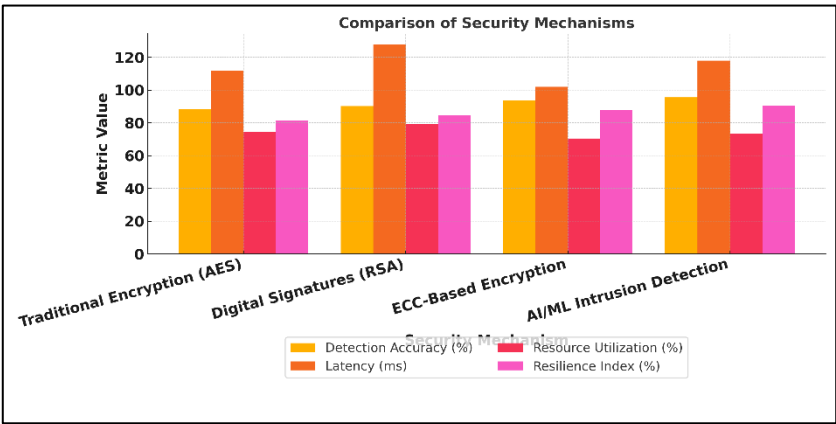


Figure 2
Performance Comparison of Cybersecurity Mechanisms across Key Metrics

With 95.6% accuracy, 118 ms of lag, and the highest resilience score of 90.4%, AI/ML attack detection is the best way to keep power systems safe in real time and adapt to changing threats.

V. Conclusion

Strong information security in an organization's power systems needs proactive, complex plans that can accurately and reliably deal with new cyber dangers. Cryptography, AI-based breach detection, and zero-trust systems are some of the most important defences. Mathematical models and attack-defense exercises help with planning ahead. These steps improve privacy, security, and availability across systems that are linked to each other. Adaptive security, fewer outages, and higher resilience can be achieved by organisations that combine technology remedies with predictive risk assessments to protect vital power system operations.

References

- [1] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, "Digital transformation: An overview of the current state of the art of research," *Sage Open*, vol. 11, no. 3 (2021).
- [2] M. S. S. Danish, "AI in energy: Overcoming unforeseen obstacles," *AI*, vol. 4, pp. 406–425 (2023).
- [3] B. Garlik, "Energy centers in a smart city as a platform for the application of artificial intelligence and the internet of things," *Applied Sciences*, vol. 12, no. 3386 (2022).
- [4] M. Dhanaraju, P. Chenniappan, K. Ramalingam, S. Pazhanivelan, and R. Kaliaperumal, "Smart farming: Internet of Things (IoT)-based sustainable agriculture," *Agriculture*, vol. 12, no. 1745 (2022).
- [5] V. Stoicescu, T. I. Bițoiu, and C. Vrabie, "The smart community: Strategy layers for a new sustainable continental framework," *Smart Cities*, vol. 6, pp. 410–444 (2023).
- [6] M. F. Rabbi, J. Popp, D. Máté, and S. Kovács, "Energy security and energy transition to achieve carbon neutrality," *Energies*, vol. 15, no. 8126 (2022).
- [7] I. Sotnyk, T. Kurbatova, Y. Romaniuk, O. Prokopenko, V. Gonchar, Y. Sayenko, G. Prause, and A. Sapiński, "Determining the optimal directions of investment in regional renewable energy development," *Energies*, vol. 15, no. 3646 (2022).
- [8] A. Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar, and V. Khetani, "Ethical hacking and penetration testing strengthening cybersecurity posture through offensive security measures," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 4, pp. 1295–1305 (2024).

- [9] V. Deshpande, D. Khubalkar, A. Dhablia, M. J. Pasha, D. Dhabliya, and Y. Gandhi, "Enhancing financial transaction security with lightweight cryptographic algorithms," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 741–751 (2024).
- [10] S. Deshmukh, B. Tiple, G. T. Chavan, M. Phatak, G. Gondhalekar, and R. B. Raut, "Exploring alternative techniques for accelerating deep learning convergence for batch normalization," *Journal of Information and Optimization Sciences*, vol. 46, no. 4-B, pp. 1165–1175 (2025), doi: 10.47974/JIOS-1900.
- [11] X. Wang, S. Li, and M. A. Rahman, "A comprehensive survey on enabling techniques in secure and resilient smart grids," *Electronics*, vol. 13, no. 2177 (2024).
- [12] U. N. Bodhale, S. M. Bhagwat, N. A. Damare, and G. J. Ingale, "Adaptive driver vigilance monitoring system for enhanced road safety," *International Journal of Advanced Computer Engineering and Communication Technology (IJACECT)*, vol. 13, no. 2, pp. 10–15 (Mar. 2025).

Received April, 2025