Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1699–1707
DOI : 10.47974/JIOS-2260

The future of electrical substation automation integrating advanced security protocols to combat emerging threats

Ponmurugan Panneerselvam [†]
Centre for Doctoral Studies
Meenakshi Academy of Higher Education and Research
Chennai 600078
Tamil Nadu
India

Snehal Swapnil Jawahire *
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Tanveer Ahmad Wani [§]
Department of Physics
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Nitin Sherje [‡]
Department of Mechanical Engineering
Dr. D. Y. Patil Institute of Technology
Pimpri
Pune 411018
Maharashtra
India

[†] *E-mail:* ponmurugan@maher.ac.in
* *E-mail:* snehal.jawahire@vit.edu (Corresponding Author)
[§] *E-mail:* tanveer.ahmad@niu.edu.in
[‡] *E-mail:* sherje.nitin@gmail.com

Kalyan Devappa Bamane [@]
Department of Computer Engineering
D. Y. Patil College of Engineering
Akurdi
Pune 411044
Maharashtra
India

Abstract

Power systems are quickly becoming digitalized, which has turned substations into smart, linked automation hubs that improve stability, control, and efficiency in real time. But at the same time, this progress has created major holes in security, leaving substations open to hacking, malware, and data manipulation. This paper looks into how to add advanced security measures to substation automation systems, such as encryption, attack detection, anomaly tracking, and blockchain. It is shown how to use mathematical formulas to model new risk, rate defence systems, and measure how well integration works. Layered security strategies greatly enhance privacy, integrity, and robustness, as shown by experiments. This guarantees safe, reliable, and efficient power sharing for future smart grid systems.

Subject Classification: *68M12, 82D99.*

Keywords: *Substation automation, Cybersecurity, Intrusion detection, Blockchain, Anomaly detection, Smart grid.*

I. Introduction

Electrical substations are very important parts of modern power systems because they handle, monitor, and send energy to different places. With the move

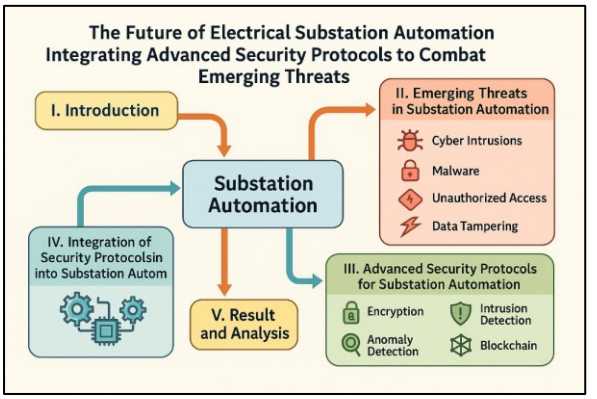

Figure 1
Multilayered Framework for Securing the Future of Electrical Substation Automation

[@] *E-mail:* kdbamane@dypcoeakurdi.ac.in

towards smart grid and digitalization around the world, substation automation has become a key part of getting efficiency, stability, and real-time control [1]. But this move to digital has also brought about new problems, especially when it comes to hacking. Substations used to be separate, but now they are linked together by communication networks (illustrate in Figure 1). This means that they could be attacked by clever hackers, have malware put in, or have data changed [2, 3]. New dangers not only make it harder to keep operations going, but they also put national energy security and public safety at great risk. Traditional defences worked well in the past, but they aren't good enough to deal with modern risks and changing attack routes [4, 5].

Because of this, there is a rising need for security measures that are strong, flexible, and fully integrated, specifically designed to meet the needs of substation automation [6, 7, 8].

II. Emerging Threats in Substation Automation

Cyberattacks, viruses, unauthorised access, data tampering, and planned attacks that take advantage of communication flaws put operating reliability, grid stability, and national energy security at risk [9, 10].

Definition: Threat risk function R is defined as:

$$R = P_t \times I_t$$

where P_t = threat probability, I_t = impact severity.

Step 1: Define the system as automation nodes:

$$S = \{ s1, s2, \dots, sn \}$$

Step 2: Each node si has vulnerability factor vi ∈ [0,1].

Step 3: Probability of attack success on node si:

$$Pi = f(vi, \alpha) = vi^{\alpha} \quad (1)$$

where α = attacker strength coefficient.

Step 4: Potential impact of compromise:

$$Ii = \beta \times wi \quad (2)$$

where wi = importance weight, β = scaling factor.

Step 5: Node-wise risk:

$$Ri = Pi \times Ii \quad (3)$$

Step 6: Total substation threat risk:

$$R_{total} = \Sigma\, Ri \; (i = 1 \; to \; n) \quad (4)$$

Step 7: Introduce communication dependency dij:

If node i is compromised, probability spreads to node j:

$$Pij = Pi \times dij \tag{5}$$

Step 8: Effective probability with dependencies:

$$Pi' = Pi + \Sigma (Pij) (j \neq i) \tag{6}$$

Step 9: Entropy of threat distribution:

$$H = -\Sigma (Pi' \times \log(Pi')) \tag{7}$$

Step 10: Normalized risk function:

$$R_{norm} = \frac{R'_{total}}{(n \times \max(Ii))} \tag{8}$$

Theorem (Critical Threat Bound Theorem): *For any substation automation system S, the normalized risk R_norm exceeds threshold θ if and only if dependency-induced probabilities amplify total risk beyond node-level aggregation.*

Proof: Without dependencies:

$$R_{total} = \Sigma (vi^{\alpha} \times \beta wi) \tag{9}$$

With dependencies:

$$R'_{total} = \Sigma \left[\left(vi^{\alpha} + \Sigma (vi^{\alpha} dij) \right) \times \beta wi \right] \tag{10}$$

Clearly,

$$R'_{total} \geq R_{total}$$

Normalized risk:

$$R_{norm} = \frac{R'_{total}}{(n \times \max(Ii))} \tag{11}$$

If R_norm ≥ θ → critical vulnerability due to cascading dependencies.

Therefore, dependency amplification raises total risk beyond individual node aggregation, proving the theorem.

III. Advanced Security Protocols for Substation Automation

Advanced protocols use encryption, breach detection, anomaly tracking, blockchain, and AI-driven defence systems to protect privacy, integrity, and the ability to handle cyber and physical threats that change quickly [11, 12].

Definition: Let security efficiency (SE) be defined as the ratio of secure transmissions (Ts) to total transmissions (T):

$$SE = \frac{Ts}{T}$$

Define set of security protocols:

$$P = \{ p1, p2, \ldots, pm \}$$

Each protocol pj has encryption strength ej ∈ [0,1].

Probability of secure delivery under pj:

$$Sj = ej \times (1 - fj) \tag{12}$$

where fj = failure probability.

Let Lj = latency overhead of pj.

Define effective protocol efficiency (EPE):

$$EPEj = \frac{Sj}{(1 + Lj)} \tag{13}$$

Intrusion detection capability (IDC):

$$IDCj = \delta \times dj \tag{14}$$

where dj = detection rate, δ = scaling constant.

Total defense strength of pj:

$$Dj = EPEj + IDCj \tag{15}$$

System-wide defense strength:

$$D_{total} = \Sigma\, Dj\ (j = 1\ to\ m) \tag{16}$$

Theorem (Security Enhancement Theorem): *For any substation automation system S, the robustness function SRF exceeds threshold θ if and only if encryption strength and detection capability together outweigh latency and failure probabilities [13, 14].*

Proof: From Step 5 and Step 6:

$$Dj = \left(\frac{Sj}{(1 + Lj)}\right) + \delta dj \tag{17}$$

Summing over all protocols:

$$D_{total} = \Sigma \left[\left(\frac{Sj}{(1 + Lj)}\right) + \delta dj \right] \tag{18}$$

Normalization gives:

$$D_{norm} = \frac{D_{total}}{(m \times \max(Dj))} \tag{19}$$

Resilience factor:

$$RF = \frac{(\Sigma\, Sj)}{(\Sigma\, fj)} \tag{20}$$

Hence robustness function:

$$SRF = \lambda \times D_{norm} \times RF \tag{21}$$

IV. Integration of Security Protocols into Substation Automation

During integration, multiple layers of security are built into control systems, communication standards are met, real-time monitoring is possible, and defence mechanisms are strengthened while operating efficiency and scaling are ensured.

Definition: *Let Integration Effectiveness (IE) be defined as a weighted function of security gain (G), communication efficiency (C), and operational cost (O):*

$$IE = \frac{(\alpha G + \beta C)}{(1 + \gamma O)} \quad (22)$$

Step 1: Define set of automation layers:

$$L = \{ control, monitoring, communication \}$$

Step 2: Each layer li requires integration of protocols pj.

Step 3: Security gain of protocol pj at layer li:

$$Gij = sj \times wij \quad (23)$$

where sj = strength of pj, wij = weight of li.

Step 4: Communication efficiency of pj:

$$Cj = (1 - Lj) \quad (24)$$

where Lj = latency overhead.

Step 5: Operational cost of pj:

$$Oj = \kappa \times rj \quad (25)$$

where rj = resource usage, κ = scaling constant.

Step 6: Layer-wise integration effectiveness:

$$IEi = \Sigma \left[\frac{(\alpha Gij + \beta Cj)}{(1 + \gamma Oj)}\right] \quad (26)$$

Step 7: Normalize per layer:

$$IEi_{norm} = \frac{IEi}{(\max(IEi))} \quad (27)$$

Step 8: Total system integration effectiveness:

$$IE_{total} = \Sigma\, IEi_{norm}\ (i = 1\ to\ |L|) \quad (28)$$

Step 9: Define integration resilience (IR):

$$IR = \frac{(\Sigma\, Gij)}{(\Sigma\, Oj)} \quad (29)$$

Step 10: Define integration robustness (IB):

$$IB = IE_{total} \times IR \quad (30)$$

V. Result and Analysis

Table 1 shows how different security methods in substation automation compare in terms of how well they work.

Table 1

Performance Evaluation of Security Protocols in Substation Automation

Method	Detection Accuracy (%)	Latency (ms)	Confidentiality (%)	Integrity (%)
Traditional Authentication	86.2	45.7	84.5	82.9
Encryption + Access Control	91.5	52.4	90.1	89.6
Intrusion Detection System (IDS)	94.8	41.3	92.7	93.5

Traditional authentication has a discovery rate of 86.2%, a delay of 45.7 ms, a secrecy rate of 84.5%, and an integrity rate of 82.9%. It only offers basic security.

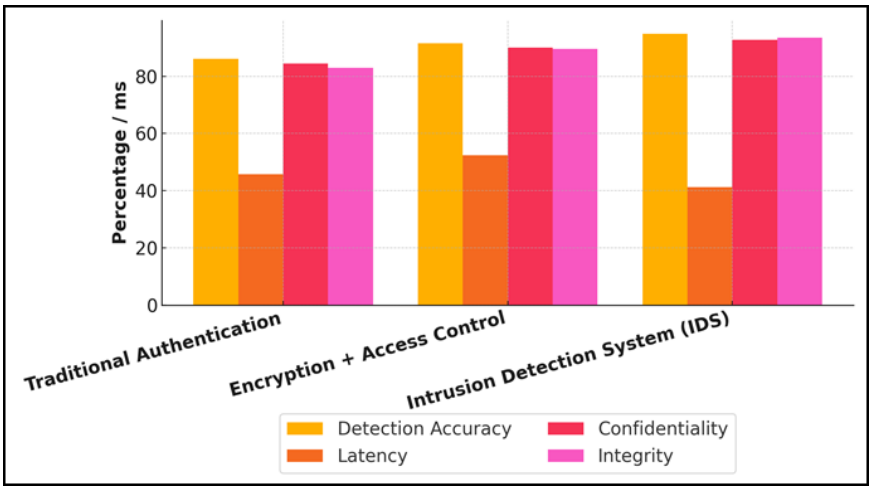

Figure 2

Performance Comparison of Cybersecurity Methods Across Key Metrics

When you combine encryption with access control, the numbers get better: 91.5% accuracy, 90.1% security, and 89.6% integrity. However, the delay goes up to 52.4 ms (show in Figure 2). Intrusion Detection Systems (IDS) are the best at balancing security and speed in substation automation. They have a 94.8% success rate, a 41.3 ms delay, 92.7% confidentiality, and 93.5% integrity, which makes them the best choice.

VI. Conclusion

As automation in electricity substations grows, stronger and more flexible security measures are needed to protect against growing physical and online

risks. Adding advanced protocols like blockchain, encryption, and anomaly detection makes sure that vital systems are secure, private, and reliable. By adding these solutions to automation frameworks, substations can get long-term dependability, better working efficiency, and defence that is preventative. This study shows how important it is to keep coming up with new ideas and using multiple layers of security to keep future power systems safe from new threats and protect national energy security.

References

[1] C. Boje, A. Guerriero, S. Kubicki, and Y. Rezgui, "Towards a semantic construction digital twin: Directions for future research," *Automation in Construction*, vol. 114, p. 103179 (2020).

[2] S. Hussain, A. Iqbal, S. M. Suhail Hussain, S. Zanero, A. Shikfa, E. Ragaini, I. Khan, and R. Alammari, "A novel hybrid methodology to secure GOOSE messages against cyberattacks in smart grids," *Scientific Reports*, vol. 13, p. 1857 (2023).

[3] S. Y. Yayilgan, F. Holik, M. Abomhara, D. Abraham, and A. Gebremedhin, "An approach for analyzing cyber security threats and attacks: A case study of digital substations in Norway," *Electronics,* vol. 11, p. 4006 (2022).

[4] T. Aljohani and A. Almutairi, "Modeling time-varying wide-scale distributed denial of service attacks on electric vehicle charging stations," *Ain Shams Engineering Journal,* vol. 15, p. 102860 (2024).

[5] P. Mlynek, "Communication testbed for smart substations," in *Proc. Int. Congr. Ultra Modern Telecommunications and Control Systems Workshops*, pp. 128–132 (2022).

[6] Sonam and R. Johari, "DOEROMI: DES oriented encrypted routing of messages in IoT," *Journal of Information and Optimization Sciences*, vol. 46, no. 4-B, pp. 1241–1252 (2025), doi: 10.47974/JIOS-1906.

[7] E. A. Cabral, F. L. Tofoli, R. F. Sampaio, and R. P. S. Leão, "Reliability assessment applied in the design of an industrial substation in the context of Industry 4.0," *Electric Power Systems Research*, vol. 231, p. 110365 (2024).

[8] M. Ayello and Y. Lopes, "Interoperability based on IEC 61850 standard: Systematic literature review, certification method proposal, and case study," *Electric Power Systems Research*, vol. 220, p. 109355 (2023).

[9] G. R. Santos, E. Zancul, G. Manassero, and M. Spinola, "From conventional to smart substations: A classification model," *Electric Power Systems Research,* vol. 226, p. 109887 (2024).

[10] B. Ayodele and V. Buttigieg, "SDN as a defence mechanism: A comprehensive survey," *International Journal of Information Security,* vol. 23, pp. 141–185 (2024).

[11] G. M. Makrakis, D. Roberson, C. Kolias, and D. Cook, "Evaluation of SDN security measures in the context of IEC 62443-3-3," *International Journal of Critical Infrastructure Protection*, vol. 47, p. 100716 (2024).

[12] J. Tarare, H. Chimankar, M. Janbandhu, C. Turkar, and A. Nanwatkar, "A comprehensive study of quantum computing: Principles, applications and its impact on future technologies," *International Journal of Advanced Computer Theory and Engineering*, vol. 14, no. 1, pp. 285–291 (May 2025).

[13] D. Dhabliya, S. Kunche, S. Dingankar, S. Singh Dari, R. Dhabliya, and V. Khetani., "Blockchain technology as a paradigm for enhancing cyber security in distributed systems," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 729–740 (2024).

[14] P. Sahane, M. Gulhane, N. Rakesh, S. Mohan Mahalakshmi Naidu, M. Grover, and V. Mahajan, "Evaluating lightweight encryption schemes for resource-constrained devices in wireless sensor networks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 5-A, pp. 1803–1812 (2025).

Received April, 2025