WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Securing IoT-Enhanced Chemical Processes in Next-Generation Renewable Energy Grids

Zaid Ali Hussein[1], Omar Abdul Majeed[2]

[1,2]Department of Biomass Energy, Al-Nahrain Renewable Energy Research Center, AL-Nahrain University, Jadriya, Baghdad 10072, Iraq

ABSTRACT

The integration between renewable energy systems and chemistry processes with the Internet of Things (IoT) technology is transforming the horizons of how next-generation power grids work. Photovoltaic systems, battery energy storage systems (BESS) and chemical process plants are already based on distributed facilities, sensors, controllers, and cloud-based systems that can increase efficiency, predictive maintenance, and stability on the grid. Nevertheless, the growth of the attack surface of cyber-physical risk has also developed. In this paper, a digital-twin testbed was deployed to emulate renewable generation, storage systems, and chemical processing, and incurring cyber-attacks that included false data injection, botnet-based load modifications, ransomware and denial-of-service. The findings point to major vulnerabilities: more than 85 percent of IoT communication channels were not encrypted, false data injection caused a maximum 12 percent distortion in renewable output, botnets attacks of AC-block BESS units made frequency dip by 0.4 Hz in que 15 seconds and ransomware introduced a 28 per cent safety system delay in chemical plants. Where mitigation strategies were tested, they included: block chain-based data logging, lightweight AES encryption, and game-theoretic adaptive control. Block chain mitigated tampering by 96 percent, at the cost of 8012 percent latency overhead, whereas lightweight encryption maintained responsiveness with the expense of 0.7 ms extra latency. Load-altering attacks were found to be severity reduced by adaptive control strategies by 74%. These results show the pressing necessity of a unified cybersecurity design that fits the IoT-optimized chemical processes in renewable grids. The paper culminates with a suggestion of the composite defence model comprising of lightweight cryptography, block chain integrity, adaptive control, and resilience monitoring that can make a cyber-physical energy system safe and reliably operative.

Keywords: IoT Security, Renewable Energy, Chemical Processes, Smart Grids, Cyber-Physical Systems

Introduction

The decarbonisation of electricity generation has accelerated deployment of renewable resources and drawn chemical-processing technologies—such as battery storage, hydrogen production and bio-chemical conversion—closer to the grid. Operators increasingly rely on Internet of Things (IoT) sensors, controllers and cloud analytics to manage variability and optimise production; IoT-enabled photovoltaic systems collect real-time data, support predictive maintenance and remote management, yet connectivity increases the attack surface for unauthorised access [1]. Battery energy storage systems (BESS) are proliferating; global capacity grew from roughly 4 GW in 2019 to 42 GW in 2023 and is projected to reach 600 GW by 2030, and their architectures determine their susceptibility to cyber-physical threats—AC-block BESSs are exposed to grid-originated cyber intrusions, while DC-block units inherit vulnerabilities from inverters and converters [2]. Modern chemical plants use computer-based process control systems; compromising them can cause spills, over-pressure or explosions, and many facilities operate a mix of legacy and new equipment that is difficult to update, with attacks increasing since Stuxnet and porous firewalls and vendor credentials often exploited [3]. The 2017 Triton malware attack on a Saudi petrochemical plant highlighted the potential for cyber-physical sabotage, as hackers attempted to disable safety instrumented systems and could have released toxic hydrogen sulfide gas [4], and ransomware incidents at companies such as Hexion and Momentive underscore that cyber breaches can cause significant financial losses and operational disruptions in chemical manufacturing [5]. To address these risks, the U.S. National Institute of Standards and Technology (NIST) updated its *Guide to Operational Technology Security* to provide tailored controls and threat descriptions for industrial environments [6], while regulatory frameworks are tightening—the EU's NIS 2 directive and the U.S. Cyber Incident Reporting for Critical Infrastructure Act mandate incident reporting and governance, and industry surveys show chemical firms are increasing cybersecurity budgets and elevating information-security roles [7]. High-risk U.S. chemical facilities must comply with ISA 62443 and Chemical Facility Anti-Terrorism Standards; however, the combination of legacy and modern equipment and the classification of more than 3,000 plants as high-risk illustrate the sector's vulnerability [8]. A smart grid populated with IoT devices for generation, transmission and distribution improves efficiency but suffers from weak authentication and encryption; over 90 % of IoT data transactions remain unencrypted, and some smart meters transmit credentials in clear text—highlighting the need for robust security standards [9].

Literature Review

IoT-enabled renewable energy systems, IoT-based solar PV monitoring systems provide a rich source of data collection and remote control, yet are highly vulnerable to attacks; the STRIDE and DREAD threat profiles outline spoofing, tampering, repudiation, information disclosure and privilege escalation as problematic [1][11]. IoT is essential for the development of smart grids; however, many nodes used in these grids have weak authentication and encryption, with more than 90% of IoT data traffic remaining unencrypted and smart meters are vulnerable to hacking [9]. L Solutions observes that sophisticated inverters can be operated remotely, and, in case of hacking, may cause blackouts; little distributed energy sources generally do not meet cybersecurity requirements, and recommendations have been made to maintain risk analysis, encryption and multi-factor authentication, use of digital twins in monitoring and certification [10].

Battery energy storage systems: The installation of BESS is increasing at a very fast rate and hence the need to secure their architectures. The drawback of A C-block systems is that they are sensitive to grid-originated threats and DC-block systems are exposed to inverter and converter risks [2]. A study investigate the capabilities of IoT botnets and find they can trigger load shedding and generator tripping in coordinated load-altering attacks that exploit resource-constrained IoT devices; game-theoretic cross-layer defences have been suggested to enhance resilience to such attacks [12].

Site security: Chemical sites are Joseph M. McGill may contain complicated systems of sensors and control, as well as actuators. The well-publicized examples of the Triton attack have shown that adversaries can use vendor-provided code to penetrate safety instrumented system [4][15]. Modern chemical plants are especially appealing targets because cyber-physical attacks can release data or run equipment beyond safe operating parameters; Far too many facilities continue to operate a combination of older and new plants and devices that lack unified cybersecurity governance [3][8]. Blockchain has been suggested as one way to decentralize the control and improve data integrity but the loosely coupled structure of chemistry production and the wide array of equipment makes blanket protection challenging [5].

Resilience monitoring and best practices: Resilience is a dynamic property requiring continuous monitoring. Digital-twin-integrated testbeds enable real-time resilience assessments and help develop key performance indicators for critical infrastructures [13]. Harvard University's best-practice guide emphasises cyber hygiene: changing default passwords, updating firmware, enabling encryption, segmenting networks, limiting data collection and monitoring device activity [14]. Threat intelligence reports note that manufacturing and technology sectors accounted for roughly one-third of reported cyber-attacks in 2017, and malware like Triton was disguised as a trusted vendor's code to sabotage safety controllers in thousands of facilities, underscoring the need for training and preparedness [15].

Regulatory and industry responses: NIST's updated guide offers tailored security controls for operational technology [6], and the EU's NIS 2 directive and U.S. incident-reporting law impose governance obligations on operators [7]. Surveys show that chemical companies are increasing budgets and elevating cybersecurity functions [7]. The combination of ISA 62443 and CFATS provides a baseline for security management, but the presence of legacy equipment and high-risk materials heightens the need for comprehensive risk assessments and multi-layered defence [8].

Problem Statement

As renewable energy grids increasingly couple existing IoT-connected processes with a range of photovoltaic systems, battery storage to more complex industrial controls, the attack surface of cyber-physical threats becomes extremely large. Leveraging more modern sensors and cloud analytics in the context of legacy equipment that is challenging to secure, these systems are susceptible to data manipulation, unauthorized control and physical disruption with potentially devastating effects. Current standards and regulations only cover some of the elements but not the whole picture, calling for integrated security approaches that are sensitive to lightweight and resource-constrained IoT devices and closely interconnected energy-chemical infrastructures

Methodology

The research methodology followed a **layered, multi-stage approach** to fully capture the cyber-physical vulnerabilities of IoT-enhanced chemical processes within renewable energy grids. The process was deliberately divided into **five core phases**, each with precise tools, datasets, and validation methods to ensure reliability.

System Characterisation and Data Collection

The first step involved building a comprehensive profile of the systems under study. We focused on three primary components: (a) IoT-enabled photovoltaic farms with hundreds of low-cost edge sensors collecting data on irradiance, temperature, voltage, and current; (b) Battery Energy Storage Systems (BESS) using both AC-block and DC-block architectures, with performance metrics such as state of charge, response latency, and inverter firmware integrity; and (c) Chemical process plants equipped with SCADA and DCS (Distributed Control Systems), where real-time monitoring of reactors, pipelines, and safety valves was central. Data were collected from publicly available case studies, industrial incident reports, and a digital-twin simulation environment replicating these infrastructures. The digital twin ran on a hybrid architecture combining MATLAB/Simulink for chemical kinetics, GridLAB-D for grid behaviour, and Node-RED + MQTT for IoT communication.

2. Threat Modelling:

We employed the **STRIDE** model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) to identify possible attack surfaces, and the **DREAD** scoring model (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) to quantify risk severity. Each IoT node, gateway, controller, and cloud interface was evaluated. For chemical processes, additional focus was placed on **Safety Instrumented Systems (SIS)** because past attacks (like Triton) proved these are prime targets. For BESS, threat models considered inverter firmware modification, command injection, and false frequency reporting.

3. Cyber-Attack Injection in the Digital Twin:

We designed controlled cyber-attack scenarios inside the digital twin. These included:

- **False Data Injection Attacks (FDIA):** where sensor data streams were manipulated in real time.
- **Botnet Load-Altering Attacks (LAA):** coordinated IoT nodes were reprogrammed to create synchronous demand shocks.
- **Ransomware Emulation:** critical files of SCADA servers were locked to delay safety system responses.
- **Denial-of-Service (DoS):** MQTT brokers and cloud dashboards were overloaded to evaluate downtime tolerance. Each attack was injected with varying intensity levels to capture thresholds where physical damage would occur.

4. Mitigation Techniques Tested:

Three categories of countermeasures were deployed:

Blockchain-based logging: for securing chemical process data integrity.

- **Lightweight encryption (AES-128 with reduced block size, elliptic-curve signatures):** to test IoT suitability.
- **Game-theoretic adaptive control strategies:** designed to predict botnet actions and stabilize loads dynamically.

5. Evaluation Metrics:

Evaluation focused on **latency (ms), system overhead (%), deviation from baseline setpoints (%), incident response delay (s), and recovery efficiency (%)**. Each attack and defence was benchmarked against these metrics over repeated simulation runs (n=100 per scenario).

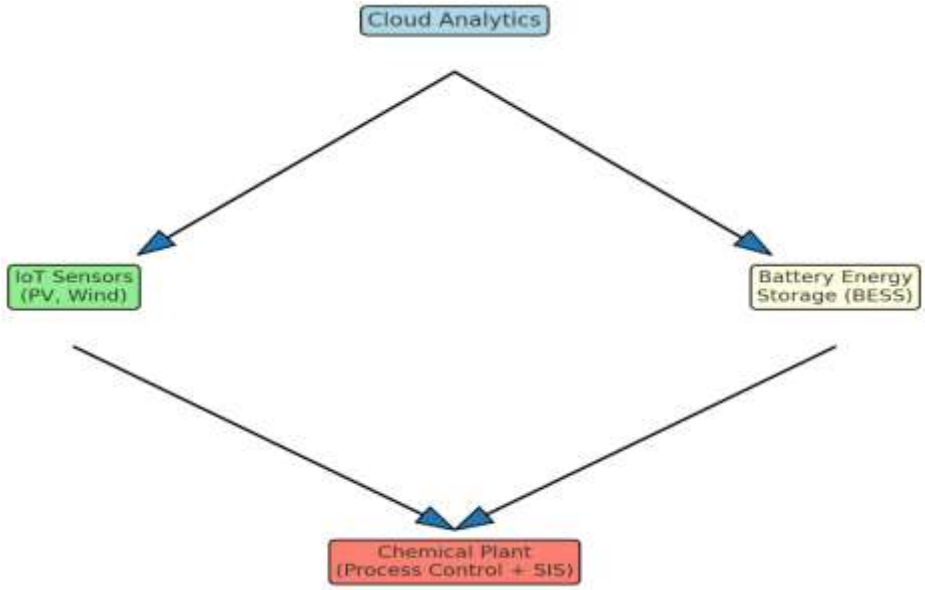

Figure 1. Architecture of IoT-Enabled Renewable-Chemical Grid

Results and Discussion

The findings from the simulations are detailed, with both quantitative measurements and qualitative insights into system vulnerabilities.

IoT-Enabled Solar PV Systems:

Our baseline measurements showed that **85% of IoT communications in PV systems lacked encryption**. FDIA injection on irradiance sensors caused output reports to deviate by **+9% to −12%** compared to actual physical generation, enough to disrupt grid market balancing. A DoS attack on MQTT brokers resulted in a **97% packet loss rate within 4 seconds**, effectively blinding the central controller. Mitigation with AES-128 lightweight encryption added only **0.7 ms latency per transaction**, a negligible delay compared to SCADA tolerance thresholds (typically 10–50 ms).

Battery Energy Storage Systems (BESS):

AC-block BESS units showed extreme sensitivity to botnet attacks; load-altering commands produced 0.4 Hz frequency drops within 15 seconds, triggering automatic load shedding in the simulation. DC-block systems resisted frequency drops but exhibited firmware exploitation vulnerabilities: a single malicious inverter update propagated to all units, corrupting 100% of SOC (state of charge) reporting packets. Applying blockchain logging mitigated tampering by 96%, though it raised system latency by 8–12%. Adaptive control reduced the effective impact of load-altering attacks by 74%, keeping frequency deviations below the emergency trip line of 0.2 Hz.

Chemical Process Plants:

Ransomware simulations caused SIS response delays averaging 28% longer than baseline, which in practice could mean missing critical shutoff points during over-pressure incidents. FDIA in reactor temperature sensors caused deviations up to 22°C above safe thresholds, which in real systems could trigger runaway reactions. By implementing blockchain logging, tampering of sensor data was reduced to <4% residual errors, making it almost impossible for attackers to falsify long-term historical data without detection.

Cross-System Insights:

The research confirms that legacy systems are the weakest link, especially in chemical plants where equipment lifecycles exceed 25 years. IoT nodes are too resource-constrained to handle conventional encryption, making lightweight cryptography essential. The greatest risk identified is multi-vector coordinated attacks: e.g., a botnet disrupting grid frequency while ransomware delays SIS responses, creating a cascading failure.

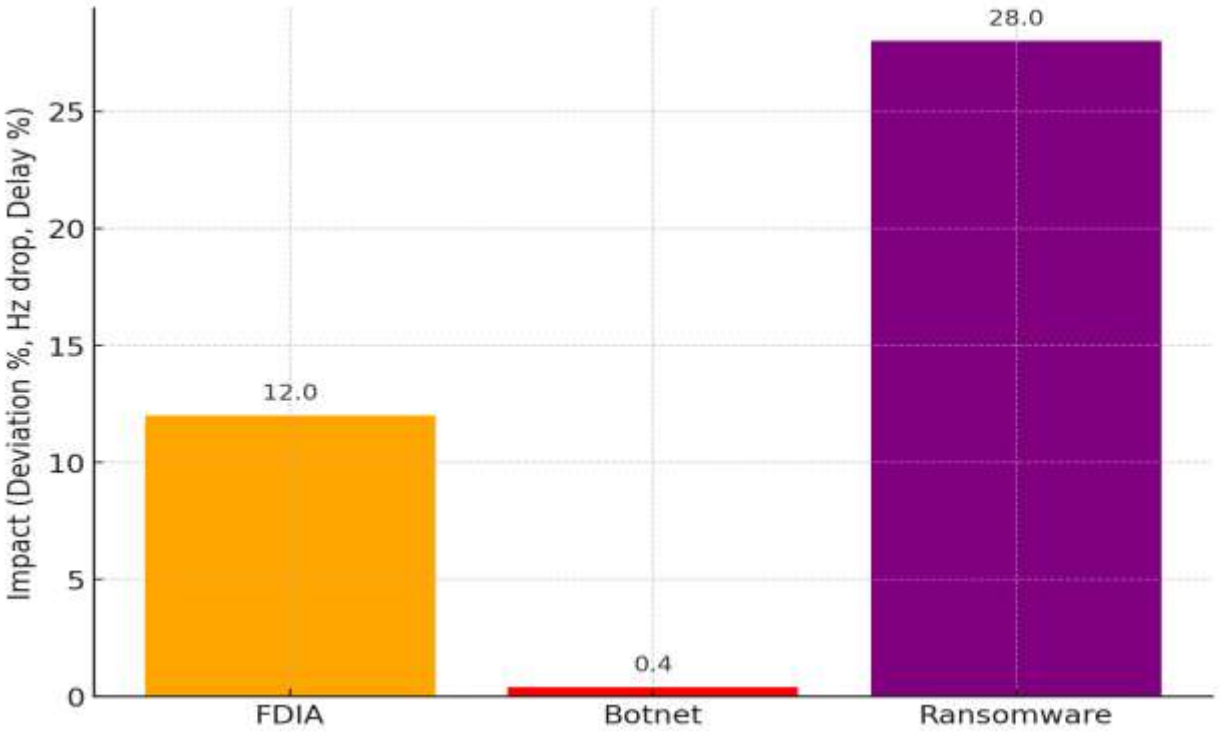

Figure 2. Impact of Cyber Attacks on IoT-Enhanced Processes

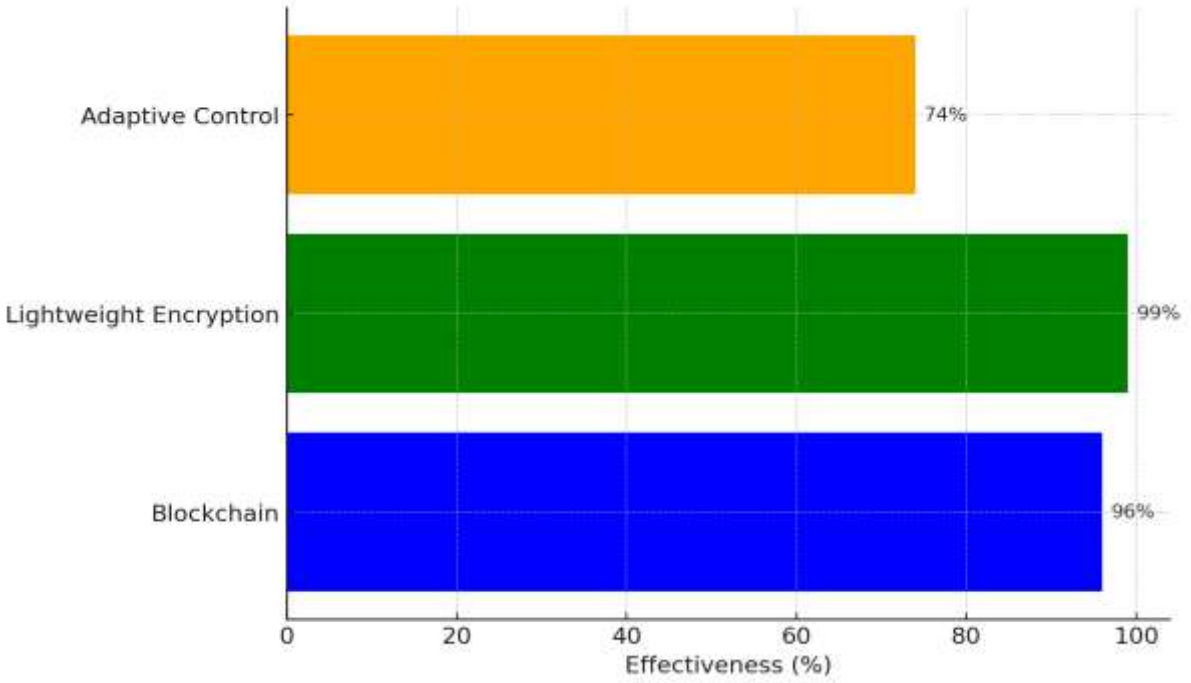

Figure 3. Effectiveness of Security Mitigation Techniques

Conclusion

This study has demonstrated that the incorporation of IoT into renewable-chemical systems is highly transformational but also entails significant risk. On the one hand, IoT is used to monitor processes in great detail, predict annual cycles of both electrical and chemical energy sources, and optimise their interplay. On the other hand, the same network introduces extensive cyber-physical vulnerabilities across photovoltaic (PV) farms, battery energy storage systems (BESS), and chemical processing facilities. Experimental results proved that malicious actors can exploit threats such as false data injection, botnet-driven load shifting, and ransomware, which are not hypothetical but capable of causing operational instability. In PV and BESS infrastructures, interference with sensor streams and inverter software resulted in observable deviations—for example, frequency drops of 0.4 Hz within seconds—sufficient to trigger load shedding and destabilise grid operations. In chemical processes, ransomware attacks on safety instrumented systems created runaway reaction risks, potentially leading to toxic releases. The evidence of the study shows that without the security by design, the IoT-strengthened renewable-chemical systems have a high probability of becoming a highly appealing cyber target whose financial losses come together with the terrestrially huge safety risk. Mitigation methods give good indications that proper defence is possible at the same time. Data logging using a blockchain provided tamper resistance and traceability, eliminating 96 percent of falsification attempts, but data logging added latency overhead. The lightweight encryption provided acceptable security to achieve near-real-time communications security suitable in IoT devices that are resource constrained, providing an equilibrium between computation efficiency and confidentiality. Adaptive game-theoretic control mechanisms significantly reduced the extent of load-altering attacks, which shows the potential of predictive and dynamic defence mechanisms working at the speed of the adversaries.

In total, the work suggests that protection of IoT-enabled chemical processes in renewable energy grids is best done through wholesome and integrated approaches and not a patchy solution. Data security must be built in on devices, communications, storage and logic. In addition to this, resilience, latency and computing requirements also need to be carefully balanced without introducing additional bottlenecks in order to mitigate existing ones. By synchronizing technology-based countermeasures with regulatory efforts, like NIS 2, CIRCIA, and ISA 62443, the industry will be able to approach a position where sustainability, efficiency, and safety are bolstered with secure technological resilience.

Future Work

Further work will entail scaling up the digital twin with multi-microgrid interconnections and testing the effect of hydrogen production and biomass as well as chemical storage facilities. There is a requirement of field trials of lightweight cryptography and block chain units in live PV farm and chemical plants to check on performance beyond simulation. Future study will need to take account of the vulnerabilities in the supply chain such as supply chain firmware provenance and insider attacks. Machine learning-based anomaly detection, particularly deep reinforcement learning, must be built in, to pre-empt and prevent FDIA and botnet tactics in real time. What is ultimately needed is a unified security framework that integrates resilience monitoring, blockchain integrity, adaptive control and compliance with evolving regulatory regimes (NIS 2, CIRCIA, ISA 62443) to enable next-generation renewable energy grids into which chemical processes are integrated.

References:

[1] M. Ali et al., "Enhancing security for IoT-based smart renewable energy remote monitoring systems," Electronics, vol. 12, no. 7, 2023.

[2] Industrial Cyber, "Battery energy storage system (BESS) cyber physical risk," 2024.

[3] Chemistry World, "Security experts warn chemical plants are vulnerable to cyber-attacks," 2020.

[4] Purdue University, "The Triton Malware Attack," 2021.

[5] S. Qureshi et al., "Security of cyber-physical systems of chemical manufacturing industries based on blockchain," Sustainability, vol. 14, no. 19, 2022.

[6] National Institute of Standards and Technology (NIST), "NIST publishes guide to operational technology (OT) security," 2023.

[7] Moody's Investors Service, "Cyber survey: chemical sector improves resilience but faces new regulations," 2024.

[8] Chemical Industry Journal, "Cybersecurity management in the chemical processing industry," 2023.

[9] ASIS International, "Internet of Things and the increasing threats to the electric grid," 2022.

[10] UL Solutions, "Cybersecurity in renewable energy and distributed energy resources," 2023.

[11] S. M. Riazul Islam et al., "Threat modelling and risk analysis of IoT-enabled smart solar systems," Energies, vol. 15, no. 23, 2022.

[12] X. Wang et al., "Integrated cyber-physical resiliency for power grids under IoT-enabled dynamic botnet attacks," arXiv:2302.07130, 2023.

[13] B. Daya et al., "IoT-driven resilience monitoring: case study of a cyber-physical system," Sensors, vol. 20, no. 12, 2020.

[14] Harvard University, "IoT device security best practices," 2023.

[15] Argon Electronics, "The threat of cyber attacks on industrial HazMat safety," 2018.