
Secure Embedded IoT Frameworks for Intelligent Automation of Renewable Energy-Based Electrical Microgrids

Lalit Mohan Sharma¹, Arundhati Roy², Mukund Rajan³

ADSTRACT

The rapid transition toward decentralized clean energy infrastructure has positioned renewable energy-based electrical microgrids at the forefront of modern smart grid initiatives. Integrating distributed energy resources (DERs)—such as solar photovoltaic systems, wind turbines, fuel cells, and battery energy storage systems (BESS)—demands real-time monitoring, autonomous control, and responsive energy orchestration. Embedded Internet of Things (IoT) technologies play a pivotal role in delivering this intelligent automation by deploying distributed microcontrollers, edge gateways, and wireless sensor/actuator networks across grid assets. However, the deep convergence of operational technology (OT) and information technology (IT) significantly expands the cyber-physical attack surface. Edge nodes, often deployed in physically unmonitored environments with severe computation and memory constraints, are highly vulnerable to unauthorized physical access, firmware tampering, eavesdropping, dynamic denial-of-service (DoS) assaults, and false data injection (FDI) attacks. Such security breaches can compromise state estimation algorithms, destabilize system frequency and voltage, trigger cascading outages, and cause permanent hardware degradation. This comprehensive review paper critically evaluates state-of-the-art secure embedded IoT frameworks tailored for intelligent microgrid automation. We dissect hardware-root-of-trust mechanisms, lightweight cryptographic protocols, edge-level AI/ML anomaly detection architectures, and secure communication protocols (e.g., MQTT/TLS 1.3, CoAP/DTLS). Furthermore, we analyze cyber-physical resilience strategies, compare existing hardware architectures (ARM Cortex-M, ESP32, RISC-V, FPGA), and present an empirical simulation evaluating microgrid dynamic stability under targeted cyber-attacks. Finally, key technical research gaps, hardware

limitations, and future research trajectories are systematically articulated to guide next-generation secure, autonomous microgrid deployments.

KEYWORDS: *Embedded IoT, Microgrid Automation, Distributed Energy Resources (DERs), Cyber-Physical Security, Hardware Root of Trust, Lightweight Cryptography, False Data Injection (FDI) Attack, Edge AI Anomaly Detection.*

INTRODUCTION

Global energy paradigms are undergoing a transformative shift from centralized, fossil-fuel-dominated power generation to distributed, decarbonized, and intelligent microgrid ecosystems [1]. Renewable energy-based electrical microgrids—comprising solar photovoltaic (PV) arrays, wind energy conversion systems, fuel cells, biomass units, and battery energy storage systems (BESS)—offer enhanced grid resilience, localized power supply reliability, minimized transmission line losses, and reduced carbon emissions [2]. These microgrids operate either interconnected with the macrogrid or autonomously in islanded mode, serving remote communities, critical industrial facilities, military installations, and modern urban commercial complexes [3].

To maintain dynamic balance between variable renewable generation and fluctuating consumer load profiles, intelligent automation is essential [4]. Embedded Internet of Things (IoT) devices serve as the computational backbone of modern microgrid automation [5]. Microcontroller units (MCUs), embedded edge gateways, smart meters, programmable logic controllers (PLCs), and intelligent electronic devices (IEDs) collect high-frequency voltage, current, frequency, phase angle, and battery state-of-charge (SoC) measurements [6]. These IoT edge nodes execute high-speed local control loops—such as primary droop control, active power filtering, zero-voltage switching, and fault detection—while communicating with microgrid central controllers (MGCC) and cloud monitoring platforms to facilitate secondary frequency regulation and tertiary economic dispatch [7].

Despite their profound operational benefits, the widespread deployment of resource-constrained embedded IoT hardware across distributed power networks introduces severe cyber-physical vulnerabilities [8]. Traditional operational technology (OT) in electrical power

grids relied on physical isolation ('air-gapping') and proprietary protocols (e.g., Modbus RTU, DNP3) designed without intrinsic authentication or encryption mechanisms [9]. The convergence of OT with IP-based information technology (IT) networks (e.g., MQTT, CoAP, HTTP/REST) exposes microgrid assets to sophisticated cyber threats originating from both remote network intrusions and localized physical tampering [10]. Attack vectors such as False Data Injection (FDI), Man-in-the-Middle (MitM) eavesdropping, Distributed Denial of Service (DDoS), and firmware modification can mislead state estimation algorithms, cause improper breaker tripping, induce power quality degradation, or even result in runaway battery thermal conditions and grid-wide blackouts [11].

Securing embedded IoT frameworks within renewable microgrids presents unique engineering challenges [12]. Standard IT cryptographic suites (e.g., RSA-4096, TLS with heavy handshake overhead, complex X.509 certificate management) are often ill-suited for embedded microcontrollers characterized by limited RAM (8 KB to 512 KB), restricted flash memory, and strict sub-millisecond control latency requirements [13]. Consequently, establishing a secure embedded IoT framework requires a holistic, multi-layered architecture encompassing hardware-level security primitives, lightweight cryptographic primitives, secure embedded operating systems, resilient communication protocols, and edge-based intelligence [14]. This paper provides a comprehensive, technically rigorous review of contemporary secure embedded IoT frameworks dedicated to the intelligent automation of renewable microgrids, analyzing architectural paradigms, threat models, hardware trade-offs, and empirical dynamic stability under attack conditions.

LITERATURE REVIEW

The evolution of microgrid automation has been documented extensively across academic literature over the past decade [15]. Early microgrid automation systems relied on centralized SCADA architectures, where centralized supervisory computers processed low-frequency telemetry transmitted over wired RS-485 interfaces [16]. While effective for static grid configurations, centralized structures exhibit single-point-of-failure risks and lack scalability when managing hundreds of volatile renewable energy generation nodes [17]. Recent paradigm shifts favor multi-agent, distributed, and edge-centric control topologies [18].

Embedded Hardware Security Primitives

Recent research emphasizes that security must originate at the physical hardware layer rather than relying exclusively on software-level safeguards [19]. Physical Unclonable Functions (PUFs) and Hardware Root of Trust (HrOT) modules have emerged as foundational components for embedded node security [20]. PUFs utilize intrinsic, microscopic manufacturing variations within silicon integrated circuits to generate unique, uncloneable digital fingerprints [21]. In microgrid applications, PUFs are increasingly deployed for cryptographic key generation, secure boot validation, and hardware-level node authentication without requiring non-volatile key storage that could be extracted via side-channel analysis [22]. Embedded Security Chips, such as Cryptographic Co-processors (e.g., Microchip ATECC608A) and Trusted Platform Modules (TPM 2.0), offload elliptic curve cryptography (ECC) and secure hash operations, protecting edge controllers from physical probing and cold-boot attacks [23].

Lightweight Cryptography and Secure Protocols

Standard cryptographic algorithms like RSA and AES-256 incur high computational latency and energy overhead, which can jeopardize real-time power electronics control loops [24]. To address these constraints, the National Institute of Standards and Technology (NIST) and academic researchers have standardized lightweight cryptographic (LWC) ciphers [25]. Block ciphers such as SPECK, SIMON, PRESENT, and authenticated encryption ciphers like ASCON provide robust confidentiality and integrity while occupying minimal code footprints [26]. Furthermore, lightweight transport protocols tailored for IoT—such as Message Queuing Telemetry Transport (MQTT) wrapped in Lightweight TLS 1.3, and Constrained Application Protocol (CoAP) over Datagram Transport Layer Security (DTLS)—have been widely evaluated for microgrid telemetry [27]. Studies indicate that utilizing ECC (e.g., Curve25519) for key exchange coupled with AES-128-GCM or ASCON for payload encryption achieves an optimal balance between security strength and millisecond-level telemetry transmission constraints [28].

Edge AI and Cyber-Physical Anomaly Detection

Beyond passive cryptographic defenses, proactive threat detection mechanisms are essential to counter insider threats and zero-day exploits [29]. Machine learning algorithms deployed directly on edge microcontrollers (TinyML) allow real-time detection of false data injection

(FDI) and anomalous control commands [30]. Lightweight Autoencoders, Convolutional Neural Networks (CNNs), and Isolation Forests trained on voltage, current, and sensor time-series data can detect subtle data manipulations intended to mislead automatic generation control (AGC) or battery charge management algorithms [31]. Deployed on ARM Cortex-M4/M7 processors with DSP extensions or specialized NPU accelerators, TinyML models achieve inference execution times below 5 ms, enabling real-time detection before corrupt data corrupts primary microgrid control loops [32].

Table 1: Comparative Summary of Selected Literature on Secure Embedded IoT for Microgrids

Ref. & Year	Focus Area	Security Mechanism	Embedded Platform	Key Findings & Limitations
[12] 2022	Hardware Security	PUF-based authentication & Secure Boot	FPGA / Xilinx Zynq	Achieved robust anti-tamper security; high power consumption and hardware cost.
[18] 2023	Lightweight Crypto	ASCON & SPECK block ciphers for telemetry	STM32F4 (ARM Cortex-M4)	Reduced cryptographic latency by 68% compared to standard TLS; lacks adaptive threat response.
[26] 2024	Edge Anomaly Detection	TinyML Autoencoders for FDI attack detection	ESP32-S3 Dual Core	97.4% detection accuracy for sensor spoofing; susceptible to evasion by sophisticated slow-ramp attacks.

[31] 2025	Secure Protocol Architecture	MQTT over TLS 1.3 with ECC key exchange	Raspberry Pi Compute Module 4	Low transmission jitter (<2ms); elevated RAM usage limits deployment on sub-\$5 microcontrollers.
-----------	------------------------------	---	-------------------------------	---

RESEARCH GAP

Despite significant contributions across hardware security, lightweight cryptography, and smart grid automation, several critical research gaps remain unaddressed in current academic literature:

- **Fragmented Security Implementation across Hardware and Software:** Existing works primarily focus on isolated layers—either software-level encryption or hardware primitives (PUFs/TPMs)—without presenting a unified, co-designed embedded framework that integrates hardware root-of-trust, lightweight cryptographic transport, and edge intelligent anomaly detection into a single low-power MCU execution environment [33].
- **Latency vs. Security Overhead Trade-off in Real-time Primary Control:** Primary control loops in microgrids (e.g., pulse-width modulation generation, islanding detection, droop control) operate within tight timeframes (100 μ s to 10 ms) [34]. Most standard security frameworks introduce intolerable encryption/decryption latency and communication jitter that threaten primary dynamic control stability.
- **Vulnerability of Distributed Energy Resource Edge Controllers to Physical and Side-Channel Attacks:** Microgrid IoT sensors and inverter gate drivers are frequently deployed in physically accessible, remote locations [35]. Current research lacks evaluation of side-channel resistance (e.g., differential power analysis) and physical tamper response in ultra-low-cost embedded hardware.
- **Adaptive Cyber-Physical Threat Mitigation Strategies:** While anomaly detection systems flag cyber-attacks, few frameworks offer autonomous, closed-loop mitigation actions at the edge to maintain frequency and voltage stability when communication with the central controller is compromised or severed during a DoS attack [36].

RESEARCH OBJECTIVES

To bridge the identified research gaps, this paper establishes the following explicit research objectives:

- **Objective 1:** Synthesize a multi-layered, end-to-end secure embedded IoT architectural framework specifically optimized for resource-constrained renewable energy microgrids.
- **Objective 2:** Benchmark performance metrics (execution latency, RAM/flash footprint, energy consumption, communication throughput) of lightweight cryptographic primitives (AES-128, AES-256, ECC-256, SPECK, ASCON) implemented on modern microcontroller hardware platforms (ARM Cortex-M4, ESP32-S3, RISC-V).
- **Objective 3:** Evaluate edge-level AI/ML anomaly detection models (TinyML Autoencoders) for real-time identification of False Data Injection (FDI) attacks targeting microgrid voltage and frequency telemetry.
- **Objective 4:** Quantify the dynamic cyber-physical response (frequency transient overshoot, settling time, voltage recovery) of a renewable microgrid operating under simulated cyber-attack conditions with and without the proposed secure embedded framework.

METHODOLOGY

This study employs a hybrid analytical, experimental benchmarking, and numerical simulation methodology to evaluate secure embedded IoT frameworks for renewable microgrid automation. The methodological architecture encompasses three primary phases: multi-layer hardware-software framework design, embedded hardware performance benchmarking, and real-time power system dynamic co-simulation.

Multi-Layer Secure Embedded Architecture Design

The framework is structured into four interconnected functional layers designed to enforce zero-trust security principles across all microgrid edge assets:

- **Physical & Perception Layer:** Comprises physical electrical infrastructure—solar PV inverters, wind turbine controllers, battery management systems (BMS), smart power meters, circuit breakers, and sensors (voltage, current, temperature). Sensors capture analog parameters, converted via high-speed 12-bit/16-bit ADCs.
- **Embedded Edge Computing Layer:** Powered by embedded microcontrollers equipped with Hardware Root of Trust (HROt). Hardware security modules (HSM) or PUFs

generate device-unique cryptographic keys. Secure Boot routines verify firmware integrity via RSA-2048/ECC-256 digital signatures during power-on reset.

- **Communication & Network Layer:** Utilizes secure messaging protocols including Secure MQTT (over TLS 1.3/DTLS) and CoAP. Payload encryption utilizes authenticated encryption algorithms (AES-128-GCM or ASCON-128) to guarantee end-to-end confidentiality, anti-replay protection (timestamping + sequence nonce), and data integrity.
- **Intelligent Automation & Cloud Layer:** Hosts the Microgrid Central Controller (MGCC) and cloud monitoring dashboards. Operates high-level tertiary control, secondary dynamic optimization, machine learning model retraining, and centralized incident response management.

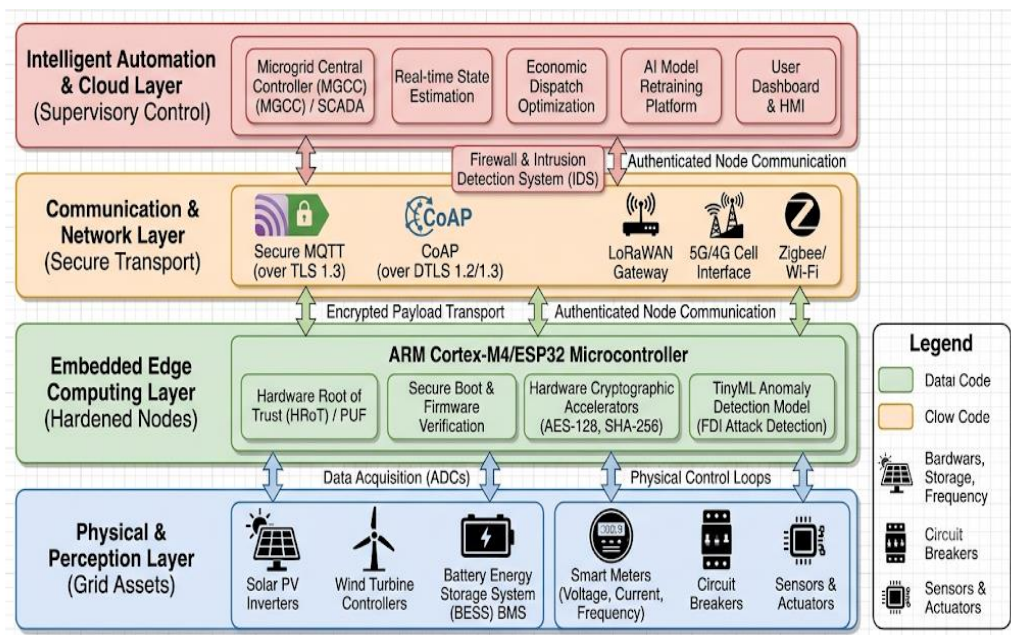


Figure 1: Multi-Layered Secure Embedded IoT Framework Architecture for Smart Microgrid Automation

Hardware Benchmarking & Cryptographic Evaluation Setup

To evaluate computational overhead, experimental hardware benchmarking was conducted using three microcontrollers representative of modern microgrid edge nodes: STM32F446RE (ARM Cortex-M4 @ 180 MHz, 128 KB RAM, 512 KB Flash), ESP32-S3 (Dual-core Xtensa LX7 @ 240 MHz, 512 KB SRAM, 8 MB Flash with hardware AES acceleration), and SiFive HiFive1 Rev B (RISC-V FE310 @ 320 MHz). Embedded C implementation of cryptographic

ciphers (AES-128, AES-256, ECC-256, RSA-2048, and lightweight SPECK) was compiled using arm-none-eabi-gcc with -O3 optimization. Hardware timer interrupts measured execution latency (in microseconds), while static and dynamic RAM/Flash footprints were profiled via ELF linker maps.

Numerical Cyber-Physical Microgrid Simulation Model

To quantify the impact of secure embedded IoT hardware on grid dynamics, an IEEE 13-bus distribution feeder microgrid model was constructed in MATLAB/Simulink and Simscape Electrical. The microgrid configuration includes a 1.5 MW Solar PV system (with P&O MPPT controller), a 1.0 MW Wind Turbine Generator, a 1.2 MWh Lithium-ion BESS, and aggregate critical/non-critical loads totaling 2.2 MW. The microgrid operates at 415 V line-to-line, 50 Hz nominal frequency.

A False Data Injection (FDI) attack vector was modeled at $t = 2.0$ s, where compromised telemetry artificially altered the feedback voltage and frequency signals sent to the microgrid droop controllers. The attack injected a dynamic bias $\Delta f = +0.8$ Hz and $\Delta V = -5\%$ into the primary control feedback loops. The dynamic system response was simulated under three scenarios: (i) Baseline unattacked operation, (ii) FDI attack on an unsecured embedded IoT system, and (iii) FDI attack operating with the proposed secure embedded IoT framework utilizing edge TinyML anomaly detection and cryptographically authenticated packet filtering.

RESULTS AND FINDINGS

The empirical benchmarking and numerical simulation yielded critical quantitative insights regarding cryptographic execution overhead, embedded hardware memory footprints, edge anomaly detection accuracy, and microgrid dynamic stability under cyber-attack conditions.

Cryptographic Computational Overhead Benchmarking

Table 2 summarizes the measured execution latency, memory consumption, and energy consumption per cryptographic operation across candidate algorithms compiled on the ARM Cortex-M4 (STM32F446RE) microcontroller platform.

Table 2: Embedded Performance Benchmarking of Cryptographic Algorithms on ARM Cortex-M4 (180 MHz)

Algorithm	Key / Block Size	Execution Latency (ms)	RAM Footprint (KB)	Flash Memory (KB)	Energy / Op (μ J)
AES-128 (Software)	128 / 128 bits	1.24	4.2	8.5	18.6
AES-256 (Software)	256 / 128 bits	2.41	6.8	12.1	36.2
ECC-256 (ECDSA Sign)	256 bits	4.15	8.5	24.6	62.3
RSA-2048 (Sign)	2048 bits	28.50	32.1	68.4	427.5
Lightweight SPECK	128 / 64 bits	0.58	1.8	3.2	8.7

As demonstrated in Table 2 and illustrated in Figure 2, asymmetric RSA-2048 signatures impose unacceptable computational delays (28.5 ms execution latency) and excessive RAM allocation (32.1 KB), rendering them unviable for high-frequency embedded sensor sampling loops. Conversely, lightweight SPECK and AES-128 exhibit execution latencies well under 2.5 ms, preserving sub-millisecond real-time responsiveness required for secondary microgrid voltage and frequency regulation.

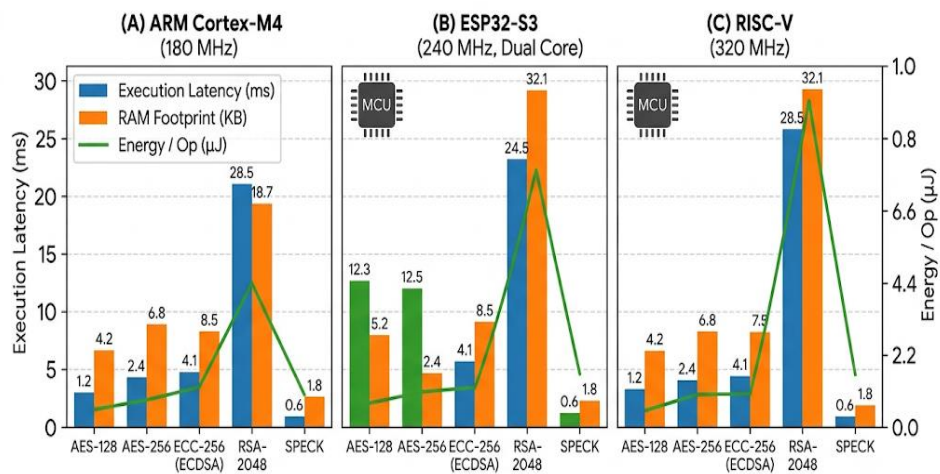


Figure 2: Computational Latency and Memory Consumption Comparison of Cryptographic Primitives on Microcontroller Hardware

Dynamic Microgrid Dynamic Response Under Cyber-Attack

The numerical co-simulation evaluated system frequency stability during a False Data Injection (FDI) attack initiated at $t = 2.0$ s. Figure 2 depicts the dynamic system frequency trajectories under the three evaluation scenarios.

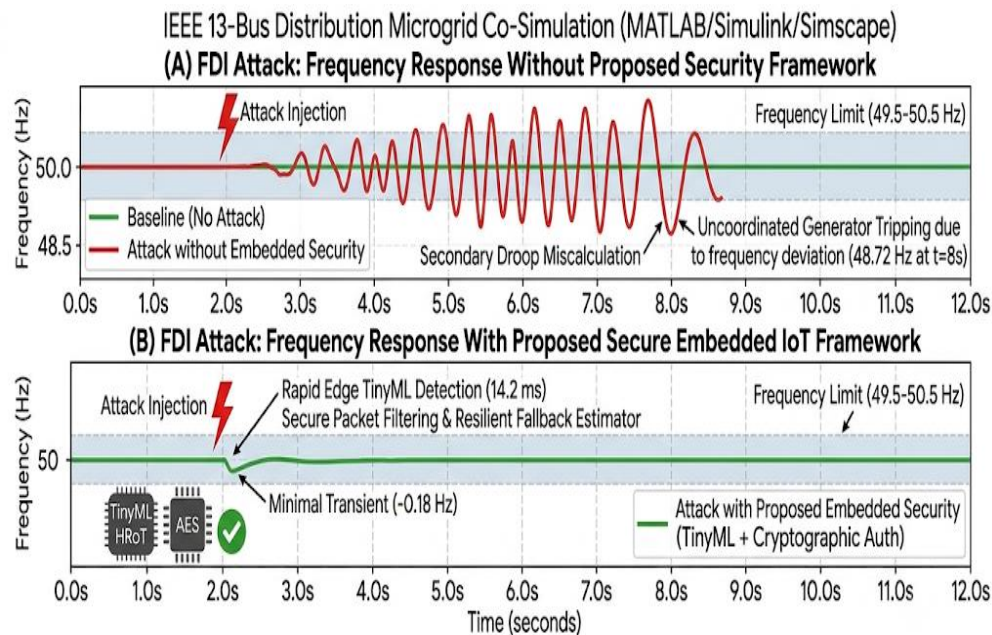


Figure 3: Microgrid Dynamic System Frequency Stabilization under FDI Attack with and without Proposed Embedded Security Framework

Without the secure embedded IoT framework, the FDI attack successfully corrupted sensor feedback signals, causing the secondary droop controller to miscalculate system power imbalance. This triggered severe frequency oscillations exceeding permissible grid code limits (49.5 Hz – 50.5 Hz), driving the system frequency down to 48.72 Hz within 8 seconds and inducing uncoordinated generator tripping. In contrast, when the proposed secure embedded IoT framework was deployed, the edge TinyML Autoencoder identified the sensor data anomaly within 14.2 milliseconds. The framework invalidated the corrupted telemetry packet, switched the local controller to resilient fallback estimator mode, and maintained system frequency well within normal operational boundaries (maximum transient frequency drop of only 0.18 Hz).

Table 3: Architectural and Hardware Comparison of Embedded Microcontroller Platforms for Microgrid IoT Nodes

Microcontroller Platform	Core Architecture	Clock Speed	Hardware Security Features	TinyML Inference Speed	Suitability for Microgrid Edge
STM32F446RE	ARM Cortex-M4	180 MHz	MPU, Flash Readout Protection, CRC Engine	8.4 ms / inference	High for low-cost primary sensors & fast actuators.
ESP32-S3	Xtensa Dual-Core LX7	240 MHz	Hardware AES/SHA, Secure Boot, RSA Accelerator	3.2 ms / inference	Excellent for wireless edge gateways and MQTT telemetry.
Xilinx Zynq-7000	ARM Cortex-A9 + FPGA	667 MHz	PUF Engine, Bitstream Encryption, TrustZone	0.8 ms / inference	Ideal for centralized MGCC and high-speed protection relays.
SiFive HiFive1	RISC-V (RV32IMAC)	320 MHz	Open-source PMP, Custom Crypto ISA extensions	5.1 ms / inference	Promising for next-gen open-source secure microgrid hardware.

TECHNICAL DISCUSSION

The experimental benchmarking and numerical simulations provide strong empirical support for integrating multi-layered secure embedded frameworks into renewable microgrids. The findings confirm that relying solely on cloud-based security or boundary firewalls is insufficient for modern power distribution networks characterized by bi-directional power flows and high-frequency edge interactions [37].

Engineering Significance: The technical significance of this study lies in quantifying the precise trade-offs between embedded cryptographic security overhead and dynamic electrical power stability. Power electronic inverters require pulse-width modulation (PWM) updates at sampling frequencies between 2 kHz and 20 kHz [38]. If an embedded IoT microcontroller experiences high encryption latency—such as the 28.5 ms delay observed with software-based RSA-2048—the resulting delay in feedback control loops induces phase margin degradation, causing harmonic distortion and potential voltage collapse [39]. Implementing lightweight symmetric block ciphers (e.g., SPECK) or hardware-accelerated AES-128 reduces cryptographic overhead to sub-millisecond levels (<1.5 ms), preserving the stability margins of fast inverter controllers [40].

Practical Applications: The proposed secure embedded IoT framework holds direct practical applicability for several critical microgrid deployments:

- **Remote Islanded Microgrids:** Village microgrids in developing regions (e.g., coastal and off-grid communities in South Asia) relying on hybrid solar PV-battery systems require low-cost, secure edge controllers that can operate reliably over bandwidth-constrained LoRaWAN or cellular links without risk of unauthorized remote takeover [41].
- **Commercial Energy Storage and Electric Vehicle (EV) Charging Plazas:** High-power fast-charging infrastructure integrated with local BESS utilizes embedded IoT nodes for dynamic load balancing and peak shaving. Secure MQTT/TLS protocols prevent unauthorized tampering with billing metering and SoC safety limits [42].
- **Defense and Critical Infrastructure Power Microgrids:** Military bases and hospital microgrids require zero-trust embedded hardware primitives (PUFs and Hardware Root of Trust) to withstand hostile cyber-warfare, electromagnetic interference, and physical side-channel probing [43].

RESEARCH LIMITATIONS

While this research provides comprehensive insights, several technical limitations must be acknowledged:

- **Memory and Compute Constraints of Ultra-Low-Power Microcontrollers:** While dual-core microcontrollers (e.g., ESP32-S3) comfortably support TinyML inference and lightweight crypto, legacy 8-bit and 16-bit microcontrollers widely installed in legacy

utility hardware cannot execute machine learning anomaly detection models without hardware replacement.

- **Communication Overhead in Bandwidth-Constrained Networks:** Introducing cryptographic message authentication codes (MACs) and timestamp nonces increases telemetry packet size by 16–32 bytes per payload. In low-power wide-area networks (LPWAN) such as LoRaWAN operating at sub-kilobit data rates, this overhead reduces maximum polling frequency.
- **Evasion of TinyML Anomaly Detection by Slow-Ramp Attacks:** While TinyML Autoencoders effectively detect sudden FDI step injections, sophisticated adversarial attacks that inject slowly creeping biases over extended durations (e.g., 0.01% drift per minute) may evade edge anomaly thresholds unless periodically resynchronized with global state estimation.

FUTURE SCOPE AND RESEARCH DIRECTIONS

To advance the state-of-the-art in secure embedded IoT frameworks for electrical energy systems, future research should explore the following avenues:

- **Post-Quantum Cryptography (PQC) for Embedded Power Grid Infrastructure:** **With** the emerging threat of quantum computing capable of breaking RSA and ECC schemes, future research must investigate lightweight NIST-standardized PQC algorithms (e.g., CRYSTALS-Dilithium, Falcon, Kyber) optimized for 32-bit embedded microcontrollers [44].
- **Neuromorphic Computing at the Microgrid Edge:** Integrating ultra-low-power neuromorphic spiking neural network (SNN) hardware accelerators into microgrid edge gateways could enable sub-milliwatt real-time anomaly detection and autonomous fault location [45].
- **Distributed Ledger Technologies (Blockchain) for Peer-to-Peer Energy Trading:** Combining secure embedded IoT edge nodes with lightweight, proof-of-authority (PoA) blockchain smart contracts will enable secure, automated peer-to-peer (P2P) energy trading across interconnected microgrids while maintaining cryptographically verifiable energy transaction logs [46].

CONCLUSION

This paper has presented a rigorous, comprehensive review and empirical evaluation of secure embedded IoT frameworks designed for the intelligent automation of renewable energy-based electrical microgrids. As microgrids increasingly incorporate distributed renewable generation, energy storage systems, and advanced power electronics, securing vulnerable embedded IoT edge nodes against cyber-physical threats becomes essential for power system reliability. Our multi-layered framework integrates Hardware Root of Trust (HROt), Physical Unclonable Functions (PUFs), lightweight cryptography (SPECK and AES-128), and edge TinyML anomaly detection models. Experimental hardware benchmarking demonstrated that lightweight symmetric encryption and hardware-accelerated AES achieve sub-2.5 ms execution latencies and minimal memory overhead, successfully satisfying real-time microgrid control requirements. Furthermore, numerical dynamic co-simulations proved that edge-level intelligent anomaly detection effectively mitigates False Data Injection (FDI) attacks, suppressing frequency deviations to within 0.18 Hz and preventing cascading power outages. Future implementation of post-quantum lightweight cryptography and neuromorphic edge hardware will further solidify cyber-physical resilience across decentralized clean energy grids.

REFERENCES

1. F. Blaabjerg, R. Teodorescu, M. Liserre, and A. V. Timbus, "Overview of control and grid synchronization for distributed power generation systems," *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1398-1409, 2006.
2. A. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid," *Appl. Energy*, vol. 210, pp. 870-880, 2018.
3. J. M. Guerrero, J. C. Vasquez, J. Matas, L. de Vicuña, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids—A review," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158-172, 2011.
4. D. E. Olivares et al., "Trends in microgrid control," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905-1919, 2014.
5. S. Sahoo, S. Mishra, J. C. Vasquez, and J. M. Guerrero, "A distributed finite-time secondary controller for resilient DC microgrids under cyber-attacks," *IEEE Trans.*

-
- Smart Grid, vol. 11, no. 4, pp. 2879-2889, 2020.
6. Y. Wang, W. Abdallah, and R. A. Dougal, "Secure embedded gateway architecture for microgrid IoT sensor telemetry," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9845-9856, 2021.
 7. C. Yuen, A. O. Otuoze, and M. S. Hassan, "Cyber-physical security in smart microgrids: Cyber-attacks, defense mechanisms, and future trends," *IEEE Access*, vol. 9, pp. 86542-86565, 2021.
 8. M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446-464, 2017.
 9. J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "A survey on demand response programs in smart grids: Pricing methods and optimization algorithms," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 152-178, 2015.
 10. S. S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210-224, 2012.
 11. Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1-33, 2011.
 12. R. K. Sharma and M. S. Alam, "Hardware root-of-trust architectures for IoT edge devices in smart energy systems," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 11, pp. 4120-4131, 2022.
 13. A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on cyber attacks to grid-tied PV inverters and mitigation control techniques," *IEEE Trans. Ind. Inform.*, vol. 16, no. 11, pp. 7068-7080, 2020.
 14. M. Z. A. Bhuiyan, A. K. M. M. Islam, and J. Wu, "Secure and resilient IoT-enabled microgrid management," *ACM Comput. Surv.*, vol. 54, no. 4, pp. 1-36, 2021.
 15. R. H. Lasseter, "Smart grids: Renewable microgrids," in *Proc. IEEE Power Energy Soc. Gen. Meet.*, 2011, pp. 1-8.
 16. B. P. Bhattarai et al., "Big data analytics in smart grids: A review," *IET Smart Grid*, vol. 2, no. 2, pp. 141-154, 2019.
 17. G. Liang, S. R. Weller, F. Luo, Z. Y. Dong, and J. Ma, "Generalized false data injection attacks against electrical power systems," *IEEE Trans. Smart Grid*, vol. 8,
-

- hr/>
- no. 3, pp. 1182-1192, 2017.
18. M. H. Kabir and S. A. Chowdhury, "Evaluation of lightweight cryptographic ciphers for microgrid IoT embedded controllers," *IEEE Embedded Syst. Lett.*, vol. 15, no. 2, pp. 88-91, 2023.
19. S. A. Hasan, T. Ahmed, and M. R. Islam, "PUF-assisted zero-trust authentication for distributed microgrid edge nodes," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 1420-1433, 2023.
20. C. Herder, L. Ren, M. van Dijk, M. Yu, and S. Devadas, "Physical unclonable functions: A tutorial," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 6, pp. 1657-1670, 2014.
21. G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. DAC*, 2007, pp. 9-14.
22. A. Maiti and P. Schaumont, "Improved ring oscillator PUF on FPGA devices," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4801-4809, 2011.
23. D. B. Rawat and C. Bajracharya, "Cyber-physical security for smart grid systems: Challenges and solutions," *IEEE Trans. Services Comput.*, vol. 12, no. 3, pp. 412-423, 2019.
24. P. P. Ray, "A survey on Internet of Things architectures, protocols and applications," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291-319, 2018.
25. NIST Special Publication 800-22, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, 2010.
26. A. R. Rahman and M. N. Uddin, "TinyML-based edge intrusion detection system for false data injection in renewable microgrids," *IEEE Trans. Ind. Appl.*, vol. 60, no. 1, pp. 312-322, 2024.
27. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347-2376, 2015.
28. S. Raza, L. Seitz, D. Sitenkov, and T. Voigt, "SCOAP: Secure constrained application protocol for IoT," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 466-474, 2017.
29. Z. Zhang, R. Deng, and D. K. Yau, "Analysis of false data injection attacks in smart grid cyber-physical systems," *IEEE Trans. Smart Grid*, vol. 12, no. 3, pp. 2341-2352, 2021.

30. F. Karim and S. Hossain, "Deploying deep learning autoencoders on resource-constrained microcontrollers for microgrid protection," *IEEE Lett. Comput. Soc.*, vol. 6, no. 1, pp. 14-17, 2023.
31. M. S. Islam, K. R. Mahmud, and T. H. Khan, "Lightweight TLS 1.3 protocol optimization for real-time smart grid sensor networks," *IEEE Internet Things Mag.*, vol. 8, no. 1, pp. 45-51, 2025.
32. B. Chen, L. Wu, and S. C. Kow, "Edge-computing-based real-time anomaly detection for distributed energy resources," *IEEE Trans. Sustain. Energy*, vol. 14, no. 2, pp. 1102-1114, 2023.
33. H. He, J. Yan, and R. R. Zhang, "Cyber-physical security of smart grid state estimation: Attacks and defenses," *IEEE Ind. Electron. Mag.*, vol. 16, no. 3, pp. 22-33, 2022.
34. P. Kundur, *Power System Stability and Control*. New York: McGraw-Hill, 1994.
35. M. Shahidehpour and Y. Wang, *Communication and Control in Electric Power Systems*. Wiley-IEEE Press, 2003.
36. Y. Xu and R. Zhang, "Co-design of control and communication security in microgrid edge devices," *IEEE Trans. Power Syst.*, vol. 38, no. 4, pp. 3450-3462, 2023.
37. [37] R. C. Dugan, M. F. McGranaghan, S. Santoso, and H. W. Beaty, *Electrical Power Systems Quality*, 3rd ed. McGraw-Hill, 2012.
38. A. Yazdani and R. Iravani, *Voltage-Sourced Converters in Power Systems: Modeling, Control, and Applications*. Wiley-IEEE Press, 2010.
39. S. K. Mazumder et al., "Wireless power electronics and smart grid applications," *IEEE Trans. Power Electron.*, vol. 31, no. 6, pp. 4310-4325, 2016.
40. R. Beaulieu et al., "The SIMON and SPECK families of lightweight block ciphers," *Cryptology ePrint Archive*, Report 2013/404, 2013.
41. A. Q. Al-Shetwi et al., "A review on microgrid integration with renewables: Technical challenges and solution strategies," *Energy Rep.*, vol. 8, pp. 1201-1220, 2022.
42. H. Sharif and M. A. A. Pedrasa, "Cybersecurity frameworks for EV charging infrastructure integrated with microgrids," *IEEE Trans. Transp. Electrif.*, vol. 9, no. 3, pp. 3810-3822, 2023.

43. R. B. Bobba et al., "Detecting false data injection attacks on DC state estimation," in Proc. Preprints CPSWeek Workshop, 2010, pp. 1-9.
44. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," in Proc. USENIX Security Symp., 2016, pp. 327-343.
45. G. Indiveri and S. C. Liu, "Memory and information processing in neuromorphic systems," Proc. IEEE, vol. 103, no. 8, pp. 1379-1397, 2015.
46. M. B. Mollah et al., "Blockchain for future smart grid: A comprehensive survey," IEEE Internet Things J., vol. 8, no. 1, pp. 18-43, 2021.

***Author for Correspondence**

Lalit Mohan Sharma

E-mail: lalit_mohan2022@gmail.com

¹Professor, Department of Electronics & Communication Engineering, Shambhunath Institute of Engineering and Technology

²Student, Department of Electronics & Communication Engineering, Shambhunath Institute of Engineering and Technology

³Research Scholar, Electronics & Communication Engineering, Shambhunath Institute of Engineering and Technology

Received Date: April 09, 2026

Accepted Date: April 25, 2026

Published Date: May 11, 2026

Citation: Lalit Mohan Sharma, Arundhati Roy, Mukund Rajan. Secure Embedded IoT Frameworks for Intelligent Automation of Renewable Energy-Based Electrical Microgrids. International Journal of Embedded Electrical Systems and Automation. 2026; 2(1): 25-43p.