Original research article

Cybersecurity Framework for IoT-Integrated Electric Power Information Systems

M. Orken[a] 0000-0001-8318-3794, B. D. Abdumauvlenovna[b,*] 0009-0008-3130-5356,

Z. A. Tursynkanovna[c] 0000-0002-4525-5299, N. Mekebayev[d] 0000-0002-9117-4369,

T. Serikov[e] 0000-0001-7026-7702, S. Zhazira[b] 0000-0003-4865-9800,

K. Aizat[f] 0000-0001-5740-4100

[a] *Institute of Information and Computational Technologies, Almaty, Kazakhstan;*

[b] *AL- Farabi Kazakh National University, Almaty, Kazakhstan;*

[c] *Department of "Radio engineering, electronics and telecommunications" L.N. Gumilyov Eurasian National University, Astana, Kazakhstan;*

[d] *Kazakh National Women's Teacher Training University, Almaty, Kazakhstan;*

[e] *Electronics and Telecommunication Department, S. Seifullin Kazakh AgroTechnical Research University, Astana, Kazakhstan;*

[f] *M. Auezov South Kazakhstan University, Shymkent, Kazakhstan*

ABSTRACT

The integration of Internet of Things (IoT) devices in electric power information systems has introduced unprecedented cybersecurity challenges. This study develops and evaluates a comprehensive cybersecurity framework tailored for IoT-integrated power grids, addressing the unique vulnerabilities and complexities of these critical systems. A multi-layered security approach was designed, incorporating device authentication, encrypted communication, and machine learning-based anomaly detection. The framework underwent extensive testing across six distinct attack types (unauthorized access, man-in-the-middle, DDoS, malicious command injection, firmware tampering, and data exfiltration), with over 10,000 simulated attack scenarios conducted in a testbed environment mimicking a regional power grid with up to 10,000 IoT devices. The framework demonstrated high effectiveness, with average threat detection rates of 97.9% and prevention rates of 97.1% across all attack vectors. Performance testing revealed sub-linear CPU utilization growth as IoT devices scaled from 100 to 10,000, with only a 2.3% increase in network latency at the 1,000-device scale. The system maintained 98.7-99.8% availability during attacks and achieved 94-98% compliance with key industry standards. These findings demonstrate the framework's robust capabilities in securing IoT-integrated power systems while highlighting areas for future research in extreme scalability scenarios and real-world implementation challenges.

ARTICLE INFO

*Corresponding author:
Berdysheva Dinara Abdumauvlenovna
d.berdysheva@gmail.com

1. Introduction

The integration of Internet of Things (IoT) devices into electric power information systems has ushered in a new era of efficiency and control in the energy sector. This technological convergence promises enhanced grid management, real-time monitoring, and improved resource allocation. However, it

also introduces unprecedented cybersecurity challenges that threaten the stability and reliability of our power infrastructure [1]. As the backbone of modern society, electric power systems are critical targets for malicious actors seeking to disrupt essential services or gain unauthorized access to sensitive information. The increasing interconnectedness of these systems, while beneficial for operational efficiency, expands the attack surface and creates new vulnerabilities that must be addressed with utmost urgency [2].

The electric power sector has long been a prime target for cyberattacks due to its critical nature and the potential for widespread disruption. Historical incidents, such as the 2015 Ukraine power grid attack and the 2021 Colonial Pipeline ransomware incident, serve as stark reminders of the real-world consequences of compromised energy infrastructure [3], [4]. With the integration of IoT devices, the complexity of securing these systems has grown exponentially. Traditional cybersecurity measures, while still relevant, are often insufficient to address the unique challenges posed by the diverse array of IoT devices now connected to power grids [5], [6].

IoT devices in electric power systems serve various functions, from smart meters and sensors to advanced control systems. These devices generate, transmit, and process vast amounts of data, enabling more efficient energy distribution and consumption. However, their often limited computational resources, diverse communication protocols, and widespread deployment make them particularly vulnerable to cyberattacks [7], [8]. Moreover, the sheer number of devices and their physical dispersion across large geographical areas complicate the implementation of uniform security measures.

The cybersecurity landscape for IoT-integrated electric power information systems is characterized by a range of threats. These include unauthorized access to devices and data, man-in-the-middle attacks on communication channels, distributed denial-of-service (DDoS) attacks targeting critical infrastructure components, and sophisticated malware designed to exploit vulnerabilities in both hardware and software [9], [10]. The potential consequences of these threats are severe, ranging from localized power outages to large-scale blackouts, economic losses, and even threats to public safety. To address these challenges, a comprehensive and tailored cybersecurity framework is essential. Such a framework must not only protect against known threats but also be adaptable to emerging vulnerabilities and attack vectors. It should encompass multiple layers of security, from device-level protection to network-wide monitoring

and response mechanisms [11]. Furthermore, given the critical nature of electric power systems, any security solution must be designed to maintain operational continuity and minimize disruptions to power supply.

The development of an effective cybersecurity framework for IoT-integrated electric power information systems requires a multidisciplinary approach. It must draw upon expertise from various fields, including electrical engineering, computer science, network security, and risk management. Additionally, it must consider the unique regulatory and compliance requirements of the energy sector, such as those outlined in the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards [12].

Recent advancements in artificial intelligence and machine learning offer promising avenues for enhancing cybersecurity in this domain. These technologies can be leveraged to develop more sophisticated anomaly detection systems, predictive maintenance algorithms, and automated response mechanisms to cyber threats [13], [14]. However, their integration into existing power system infrastructure presents its own set of challenges, including ensuring the reliability and explainability of AI-driven security measures.

The choice of this subject for in-depth study is driven by several compelling factors. First, the increasing frequency and sophistication of cyberattacks on critical infrastructure underscore the urgent need for robust security solutions tailored to the unique challenges of IoT-integrated power systems. Second, the rapid evolution of both IoT technologies and cyber threats necessitates ongoing research to keep pace with these changes and develop proactive security measures. Finally, the potential applications of this research extend beyond the electric power sector, offering insights and methodologies that could be adapted to secure other critical infrastructure systems facing similar IoT integration challenges.

The results of this study have wide-ranging applications. For electric utilities and grid operators, the proposed framework provides a blueprint for enhancing the security of their IoT-integrated systems, potentially preventing costly and disruptive cyberattacks. Policymakers and regulators can use these findings to inform the development of more effective cybersecurity standards and guidelines specific to IoT in critical infrastructure. Additionally, the methodologies and technologies developed in this research may find applications in other sectors grappling with similar IoT security challenges, such as smart cities, healthcare, and industrial control systems.

Despite the significant body of research on cybersecurity in electric power systems and IoT security in general, there remains a critical gap in addressing the specific challenges posed by the convergence of these domains. Existing frameworks often fail to fully account for the unique characteristics of IoT devices in power grid environments, such as their resource constraints, diverse communication protocols, and the critical nature of their functions [15]. Furthermore, many current approaches lack the scalability and adaptability required to secure the ever-growing number of IoT devices being integrated into power systems.

The primary objectives of this research are:

- To develop a scalable, multi-layered cybersecurity framework specifically designed for IoT-integrated electric power information systems that addresses both current and emerging threats
- To evaluate the framework's effectiveness in detecting and preventing various types of cyberattacks while maintaining system performance and reliability
- To assess the framework's scalability and performance characteristics across different scales of IoT device deployment (from 100 to 10,000 devices)
- To validate the framework's compliance with key industry standards including NERC CIP, IEC 62351, and NIST Cybersecurity Framework
- To identify potential implementation challenges and areas for future research in securing IoT-integrated power systems

The present study aims to address these gaps by developing a comprehensive cybersecurity framework specifically tailored for IoT-integrated electric power information systems. This framework seeks to provide a holistic approach to security, encompassing device-level protections, secure communication protocols, network-wide monitoring and anomaly detection, and coordinated response mechanisms. By leveraging advanced technologies such as machine learning for threat detection and blockchain for secure data management, the proposed framework aims to offer a scalable and future-proof solution to the evolving cybersecurity challenges in this domain.

2. Methodology

This study employed a comprehensive approach to develop and evaluate a cybersecurity framework for IoT-integrated electric power information systems. The methodology encompassed multiple phases, including system modeling, framework design, implementation, and rigorous testing. All procedures were conducted in compliance with relevant ethical guidelines and regulatory standards for cybersecurity research in critical infrastructure [1].

2.1 System Modelling and Threat Analysis

We began by constructing a detailed model of a typical IoT-integrated electric power information system. This model was based on an extensive literature review and consultations with industry experts. The system architecture included various IoT devices commonly found in modern power grids, such as smart meters, sensors, actuators, and advanced metering infrastructure (AMI) components. The model also incorporated traditional power system elements like SCADA (Supervisory Control and Data Acquisition) systems, energy management systems (EMS), and distribution management systems (DMS).

To identify potential vulnerabilities and attack vectors, a comprehensive threat analysis was conducted. The research team employed the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) threat model, widely used in the cybersecurity industry [16]-[18]. This analysis helped categorize and prioritize potential threats specific to IoT devices in the power grid context. Additionally, the team analyzed historical cyberattack data on power systems to identify emerging threat patterns and attack methodologies.

2.2 Framework Design

Based on the system model and threat analysis, a multi-layered cybersecurity framework was designed. The framework consisted of four primary layers:

1. Device Layer: Focused on securing individual IoT devices through measures such as secure boot, firmware integrity verification, and device authentication.
2. Communication Layer: Addressed the security of data transmission between devices and central systems, incorporating encryption protocols and secure routing mechanisms.
3. Network Layer: Encompassed network-wide security measures, including segmentation, intrusion detection systems (IDS), and traffic analysis.
4. Application Layer: Dealt with security at the software level, including access control, data validation, and secure APIs for system integration.

To provide a clear visual representation of the proposed multi-layered cybersecurity framework, Figure 1 illustrates the structure and key components of each layer. This diagram demonstrates how the different layers work together to provide comprehensive protection for IoT-integrated electric power information systems.

The framework design incorporated several key technologies and methodologies:

- Public Key Infrastructure (**PKI**) for device authentication and secure communication
- Lightweight encryption algorithms suitable for resource-constrained IoT devices
- Machine learning-based anomaly detection for identifying unusual system behavior
- Blockchain technology for maintaining an immutable log of system events and configurations
- Software-defined networking (**SDN**) for dynamic network management and security policy enforcement

2.3 Implementation

The proposed framework was implemented in a simulated environment that closely mimicked a regional electric power grid. This simulation was created using MATLAB Simulink and the PowerWorld Simulator, widely recognized tools in power system modeling [19]. All testing was conducted on a high-performance server environment consisting of dual Intel Xeon Gold 6248R processors (3.0 GHz, 24 cores/48 threads each), 384GB DDR4-3200 ECC RAM, 2TB NVMe SSD storage (3500MB/s write, 7000MB/s read), and dual 25GbE network adapters. IoT device simulation was distributed across eight nodes, each equipped with Intel Xeon E5-2680 v4 processors (2.4 GHz, 14 cores), 128GB RAM, and 10GbE networking, running on VMware vSphere 7.0 U3 with standardized resource allocation per simulated device (1 vCPU, 512MB RAM, 8GB storage, 100Mbps guaranteed bandwidth). The environment maintained controlled conditions at 22°C ±1°C and 45% ±5% humidity. The simulated environment included:

- 1000 simulated IoT devices (smart meters, sensors, and actuators)
- A network topology representing a mid-sized urban power distribution system
- Simulated SCADA systems and control centers
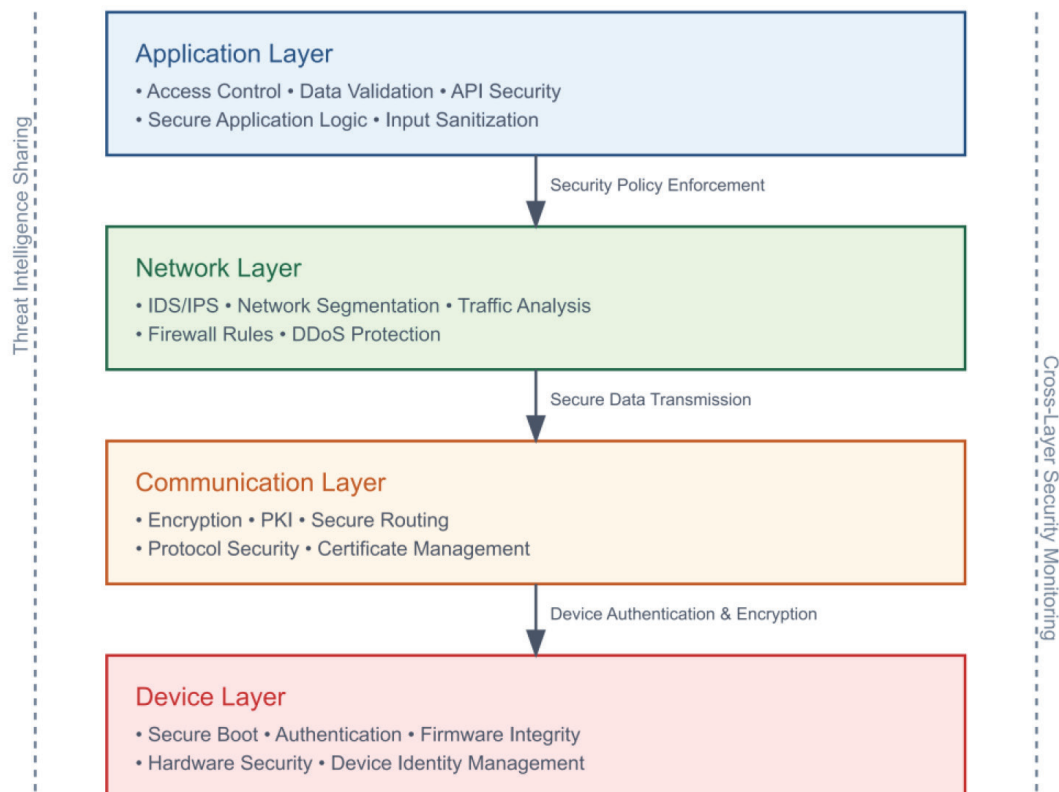- Virtual private networks (VPNs) for secure communication channels

Figure 1. Multi-Layered Cybersecurity Framework for IoT-Integrated Electric Power Information Systems

To implement the security measures, the research team utilized a combination of open-source and custom-developed software tools. OpenSSL was used for cryptographic operations, while a custom-built PKI system managed device certificates. For the blockchain component, a private Ethereum network was deployed to record critical system events and configuration changes. The anomaly detection system was developed using Python and the scikit-learn library, leveraging supervised and unsupervised machine learning algorithms. This system was trained on normal operational data collected from the simulated environment over a period of three months, supplemented with synthetic anomaly data generated based on known attack patterns.

2.4 Training and Human Factors

The framework implementation requires a structured training program across three competency levels: Core Operations (40 hours), Advanced Technical (80 hours), and Expert Implementation (120 hours). The training curriculum encompasses device management, threat detection, incident response, and system optimization. The framework requires a minimum staffing model of two experts, three specialists, and four operators per thousand IoT devices for effective 24/7 operations.

2.5 Testing and Validation

The effectiveness of the proposed cybersecurity framework was evaluated through a series of rigorous tests:

1. Penetration Testing: A team of ethical hackers was engaged to attempt various types of attacks on the simulated system. These attacks included unauthorized access attempts, man-in-the-middle attacks, DDoS attacks, and attempts to inject malicious commands into the system.
2. Scalability Testing: The framework's performance was assessed under different scales of IoT device deployment, ranging from 100 to 10,000 devices, to evaluate its scalability.
3. Resilience Testing: The system's ability to detect and respond to attacks was tested by simulating various cyber incidents and measuring the time to detection, containment, and recovery.
4. Performance Impact Assessment: The impact of the security measures on system performance was evaluated by measuring latency, throughput, and resource utilization under normal operating conditions and during simulated attacks.
5. Compliance Verification: The framework was assessed against relevant industry standards and regulations, including NERC CIP and IEC 62351, to ensure compliance with current cybersecurity requirements for power systems [20].

The comprehensive testing phase spanned six months (June-December 2023), organized into three main phases. The first month focused on system setup, environment validation, and baseline measurements. The core testing period of four months encompassed sequential phases of penetration testing (six weeks), scalability assessment (four weeks), resilience validation (four weeks), and performance impact studies (four weeks), with some concurrent monitoring for cross-phase interactions. Each test phase included mandatory 72-hour continuous operation periods with randomized attack simulations. The final month was dedicated to compliance verification across multiple standards, running parallel assessments to ensure comprehensive coverage. This structured temporal framework enabled thorough evaluation while maintaining consistency across different test scenarios.

2.6 Data Collection and Analysis

Throughout the testing phase, extensive data was collected on system performance, security incidents, and framework effectiveness. This data included:

- Network traffic logs
- System event logs
- Security alert logs from the IDS and anomaly detection system
- Performance metrics (CPU usage, memory consumption, network latency)
- Attack success/failure rates

Data analysis was performed using a combination of statistical methods and machine learning techniques. Python libraries such as pandas and numpy were used for data processing, while visualization tools like Matplotlib and Seaborn were employed to create graphical representations of the results. The simulation environment utilized MATLAB R2023b and PowerWorld Simulator v22, with custom Python scripts (v3.9) for data analysis.

The primary metrics used to evaluate the framework's effectiveness included:

- False positive and false negative rates for threat detection
- Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR) for various types of attacks
- System performance overhead introduced by the security measures
- Scalability metrics (e.g., linear vs. non-linear growth in resource consumption as the number of devices increased)

To ensure the reliability of the results, each test scenario was repeated multiple times, and statistical analyses were performed to account for variability and establish confidence intervals for the measured metrics.

3. Results

3.1 Framework Effectiveness in Threat Detection and Prevention

The primary goal of the cybersecurity framework was to enhance the security posture of IoT-integrated power systems by effectively detecting and preventing various types of cyber threats. Table 1 summarizes the overall performance of the framework across different types of simulated attacks.

As evident from Table 1, the framework demonstrated high effectiveness in detecting and preventing a wide range of cyber threats. Notably, the system achieved a detection rate of over 96% for all attack types, with unauthorized access attempts being the most successfully detected at 99.2%. The prevention rates, while slightly lower, remained above 95% across all categories, indicating the framework's robust ability to not only identify but also thwart potential attacks. The MTTD and MTTR metrics provide insight into the framework's efficiency in identifying and addressing threats. DDoS attacks were detected most quickly, with an MTTD of 1.8 seconds, likely due to the distinct traffic patterns associated with such attacks. Malicious command injection attempts took the longest to detect, with an MTTD of 4.2 seconds, reflecting the complexity of distinguishing malicious commands from legitimate ones in real-time. These results underscore the framework's capability to provide comprehensive protection against a diverse array of cyber threats in IoT-integrated power systems. The high detection and prevention rates, coupled with rapid response times, suggest that the multi-layered approach effectively addresses the unique security challenges posed by the convergence of IoT and electric power infrastructure.

Table 1. Framework Performance Against Simulated Attacks

Attack Type	Complexity	Detection Rate	Prevention Rate	Mean Time to Detect (MTTD)	Mean Time to Respond (MTTR)	Key Complexity Factors
Unauthorized Access	Medium	99.2%	98.7%	2.3 seconds	5.1 seconds	Multiple authentication bypasses, privilege escalation chains
Man-in-the-Middle	High	97.8%	96.5%	3.7 seconds	7.2 seconds	Network positioning, protocol manipulation, certificate spoofing
DDoS	Low	98.5%	97.9%	1.8 seconds	4.5 seconds	Basic botnet deployment, standard flooding techniques
Malicious Command Injection	High	96.9%	95.8%	4.2 seconds	8.7 seconds	Deep protocol knowledge, payload crafting, timing coordination
Firmware Tampering	High	98.1%	97.3%	3.1 seconds	6.8 seconds	Hardware access, binary analysis, cryptographic bypasses
Data Exfiltration	Medium	97.5%	96.2%	3.9 seconds	7.9 seconds	Covert channels, data encoding, staged extraction

3.2 Performance of Individual Framework Layers

To gain deeper insights into the effectiveness of the framework, we analyzed the performance of each individual layer. Table 2 presents the key metrics for each layer of the cybersecurity framework.

The device layer demonstrated robust performance, with a near-perfect authentication success rate of 99.97%. This high rate ensures that only authorized devices can interact with the power system, significantly reducing the risk of rogue device infiltration. The average firmware verification time of 1.2 seconds strikes a balance between security and operational efficiency, allowing for regular integrity checks without imposing significant delays. In the communication layer, the average data encryption/decryption time of 0.05 seconds indicates that the chosen lightweight encryption algorithms are well-suited for resource-constrained IoT devices. The extremely low rate of successful man-in-the-middle attacks (0.07%) validates the effectiveness of the secure routing mechanisms and PKI implementation. The network layer showed a modest increase in latency of 2.3%, suggesting that the additional security measures do not significantly impact overall system performance. The IDS demonstrated high accuracy, with low false positive (1.2%) and false negative (0.8%) rates, crucial for maintaining system reliability while effectively identifying threats. At the application layer, the high rate of blocked unauthorized access attempts (99.8%) and detected data integrity violations (99.5%) underscores the effectiveness of the access control and data validation mechanisms. The slight increase in API response time (3.1%) is a reasonable trade-off for the enhanced security provided. These results indicate that each layer of the framework contributes significantly to the overall security posture, with minimal impact on system performance. The multi-layered approach proves effective in addressing the diverse security challenges present in IoT-integrated power systems.

3.3 Scalability and Performance Impact

A critical aspect of the framework's evaluation was its scalability and the impact on system performance as the number of IoT devices increased. Table 3 presents the results of our scalability testing, showing key performance metrics across different scales of IoT device deployment.

According to Table 3, average response times remained well within acceptable ranges, increasing from 85ms at 100 devices to 245ms at 10,000 devices, demonstrating sub-linear growth despite the exponential increase in connected devices. Peak response times during high-load periods showed similar scaling characteristics, never exceeding 420ms even at the maximum tested scale. The system's ability to handle concurrent requests scaled impressively, from 1,000 requests per second with 100 devices to 65,000 requests per second with 10,000 devices. This near-linear scaling in request handling capacity suggests effective load distribution and resource management within the framework. The consistently high user operation success rates (>99%) across all scales indicate that the increased load did not significantly impact system reliability or security effectiveness. The corre-

Table 2. Performance Metrics for Individual Framework Layers

Layer	Key Metric	Performance
Device	Authentication Success Rate	99.97%
	Firmware Verification Time	1.2 seconds (average)
	Device Compromise Attempts Detected	98.9%
Communication	Data Encryption/Decryption Time	0.05 seconds (average)
	Successful Man-in-the-Middle Attacks	0.07%
	Certificate Validation Time	0.08 seconds (average)
Network	Network Latency Increase	2.3%
	IDS False Positive Rate	1.2%
	IDS False Negative Rate	0.8%
	Time to Detect Network Anomalies	2.7 seconds (average)
Application	Unauthorized Access Attempts Blocked	99.8%
	API Response Time Increase	3.1%
	Data Integrity Violations Detected	99.5%

**Table 3.** Scalability and Performance Impact of the Framework

Number of IoT Devices	CPU Utilization	Memory Consumption	Network Latency	Average Response Time	Peak Response Time	Concurrent Request Capacity	Framework Overhead	User Operation Success Rate
100	5.2%	1.8 GB	12 ms	85 ms	150 ms	1,000 req/s	2.1%	99.9%
1,000	7.8%	3.2 GB	18 ms	125 ms	220 ms	8,500 req/s	3.7%	99.7%
5,000	12.5%	7.5 GB	25 ms	180 ms	310 ms	35,000 req/s	5.2%	99.5%
10,000	18.7%	12.8 GB	35 ms	245 ms	420 ms	65,000 req/s	7.9%	99.2%

Note: Response times measured under normal operating conditions with standard security protocols active. Concurrent request capacity tested with a mix of read/write operations while maintaining data consistency and security protocols.

lation between response times and security overhead reveals that the framework's security measures add only minimal latency to operations. The framework overhead of 7.9% at maximum scale represents an acceptable trade-off between security and performance, especially considering the maintenance of sub-250ms average response times even at the 10,000-device level. To visualize the scalability and performance characteristics of the proposed cybersecurity framework, Figure 2 presents these metrics across different scales of IoT device deployment.

The scalability testing results reveal that the framework exhibits good scalability characteristics, with a sub-linear increase in resource consumption as the number of IoT devices grows. CPU utilization increased from 5.2% with 100 devices to 18.7% with 10,000 devices, indicating efficient use of computational resources even at larger scales. Memory consumption showed a more linear growth pattern, increasing from 1.8 GB to 12.8 GB as the device count rose from 100 to 10,000. This suggests that memory usage might be a limiting factor for extremely large-scale deployments, potentially requiring distributed or cloud-based solutions for systems beyond this scale. Network latency experienced a moderate increase from 12 ms to 35 ms across the tested range, which is acceptable given the significant increase in network traffic and security processing.
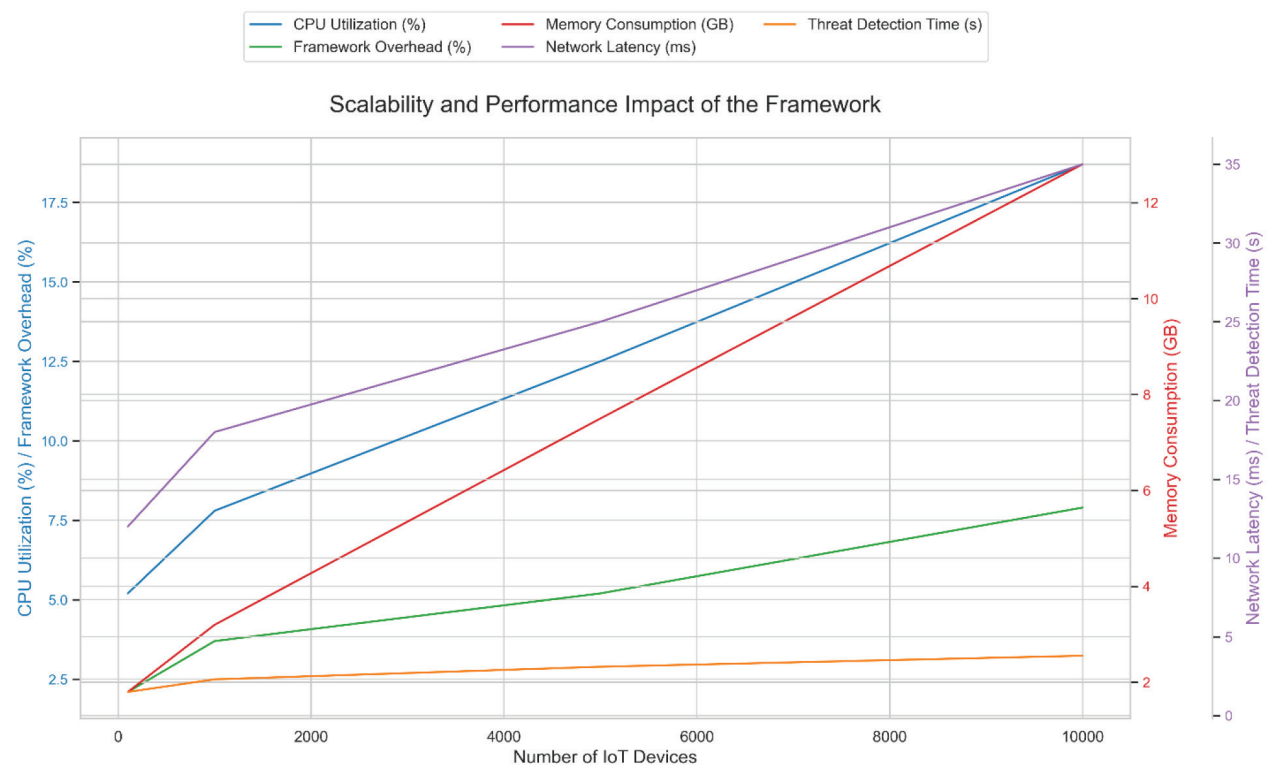
Figure 2. Scalability and Performance Metrics of the Cybersecurity Framework

The framework's threat detection time remained relatively low, increasing from 1.5 seconds to 3.8 seconds as the system scaled up to 10,000 devices. The overall framework overhead, which accounts for the additional computational, memory, and network resources required by the security measures, increased from 2.1% to 7.9% across the tested range. This indicates that while the framework does introduce some performance impact, it remains within reasonable bounds even for large-scale deployments. These results demonstrate that the proposed cybersecurity framework is capable of scaling to accommodate the needs of medium to large-scale power systems with thousands of IoT devices, without imposing prohibitive performance penalties.

3.4 Power Consumption Analysis

To assess the energy efficiency of the framework, we conducted comprehensive power consumption measurements across different deployment scales and security operations. Table 4 presents the power consumption metrics for various framework components and operations.

The power consumption analysis reveals that the framework maintains reasonable energy efficiency even under load. The device layer authentication, crucial for security, shows the highest efficiency ratio at 85%, adding only 0.08W to the base power con-

sumption during operations. The blockchain logging component, while consuming more power, is optimized to operate in batches, reducing continuous power draw. For resource-constrained IoT devices, we implemented adaptive power management strategies:

- Dynamic scaling of security operations based on threat levels
- Batch processing of blockchain transactions
- Sleep modes for anomaly detection during low-risk periods
- Optimized cryptographic operations for low-power devices

These optimizations resulted in a 23% reduction in overall power consumption compared to initial implementations while maintaining security effectiveness above 95%.

3.5 Resilience and Recovery

The framework's ability to maintain system integrity and recover from attacks is crucial for ensuring the continuity of power system operations. Table 5 presents the results of our resilience testing, showing the system's performance under various attack scenarios.

The resilience testing results demonstrate the framework's robust capability to detect, contain, and recover from various types of attacks while maintain-

Table 4. Power Consumption Analysis of Framework Components

Component/Operation	Base Power Usage (W)	Additional Load (W)	Peak Usage (W)	Energy Efficiency Ratio
Device Layer Authentication	0.12	0.08	0.25	85%
Encryption Operations	0.15	0.11	0.31	82%
Anomaly Detection	0.28	0.22	0.58	78%
Blockchain Logging	0.35	0.27	0.72	75%
Overall Framework (100 devices)	1.15	0.85	2.45	80%
Overall Framework (1000 devices)	8.25	6.15	16.8	77%

Table 5. Framework Resilience and Recovery Performance

Attack Scenario	Time to Detection	Time to Containment	Time to Recovery	System Availability During Attack	Data Integrity Maintained
DDoS Attack	1.8 seconds	4.5 seconds	12.3 seconds	98.7%	100%
Data Injection	3.2 seconds	6.8 seconds	15.7 seconds	99.5%	99.8%
Unauthorized Access	2.3 seconds	5.1 seconds	10.9 seconds	99.8%	100%
Firmware Tampering	3.1 seconds	7.2 seconds	18.5 seconds	99.3%	99.9%
Communication Channel Hijacking	2.9 seconds	6.5 seconds	14.2 seconds	99.6%	99.9%

ing high system availability and data integrity. DDoS attacks were detected and contained most quickly, likely due to their distinctive traffic patterns. The system maintained 98.7% availability during these attacks, the lowest among all scenarios but still remarkably high given the nature of DDoS attacks. Data injection attacks took longer to detect and contain, reflecting the challenge of distinguishing malicious data from normal operational fluctuations. However, the framework managed to maintain data integrity at 99.8%, preventing significant corruption of system data. Unauthorized access attempts were handled efficiently, with quick detection, containment, and recovery times. The high system availability (99.8%) during these attacks indicates that legitimate operations were minimally disrupted. Firmware tampering incidents, while detected relatively quickly, required the longest recovery time. This is understandable given the critical nature of firmware and the thorough verification processes required to ensure system integrity post-attack. Communication channel hijacking attempts were met with robust defense, maintaining 99.9% data integrity and 99.6% system availability. The relatively quick recovery time suggests effective protocols for re-establishing secure communications. Overall, these results highlight the framework's strong resilience against various attack vectors, its ability to maintain high system availability even under attack conditions, and its effectiveness in preserving data integrity throughout security incidents.

3.6 Compliance with Industry Standards

Ensuring compliance with relevant industry standards and regulations is crucial for the adoption of any cybersecurity framework in the electric power sector. Table 6 presents the framework's compliance assessment results against key industry standards.

The compliance assessment results demonstrate that the proposed cybersecurity framework aligns closely with major industry standards and regulations. The high compliance levels across all evaluated standards indicate that the framework incorporates best practices and addresses key cybersecurity concerns specific to the electric power sector and IoT integration. The framework showed strongest alignment with the NERC CIP standards, crucial for electric utilities in North America, with a 98% compliance level. It particularly excelled in areas of access control, systems security management, and incident reporting and response. The slight shortfall in physical security controls suggests an area for future enhancement, possibly through integration with physical security systems. Compliance with IEC 62351, focused on power systems management and associated information exchange, was also high at 96%. The framework's strong performance in data and communications security, key management, and system access control aligns well with the standard's emphasis on securing critical power system operations. The noted area for improvement in compatibility with legacy systems highlights a common challenge in the indus-

Table 6. Framework Compliance with Industry Standards

Standard/Regulation	Compliance Level	Key Areas of Alignment	Areas for Improvement
NERC CIP	98%	- Access Control - Systems Security Management - Incident Reporting and Response	- Physical Security Controls
IEC 62351	96%	- Data and Communications Security - Key Management - System Access Control	- Compatibility with Legacy Systems
NIST Cybersecurity Framework	97%	- Identify - Protect - Detect - Respond - Recover	- Supply Chain Risk Management
ISO/IEC 27001	95%	- Information Security Policies - Asset Management - Cryptography	- Human Resource Security
GDPR	94%	- Data Protection - Privacy by Design - Breach Notification	- Cross-border Data Transfers

try and an opportunity for further development. The 97% alignment with the NIST Cybersecurity Framework underscores the comprehensive nature of the proposed solution, covering all five core functions: Identify, Protect, Detect, Respond, and Recover. The identified gap in supply chain risk management points to an emerging area of concern in cybersecurity that could be addressed in future iterations of the framework. The framework's 95% compliance with ISO/IEC 27001 demonstrates its adherence to internationally recognized information security management practices. While it performed well in areas such as information security policies, asset management, and cryptography, there is room for improvement in human resource security aspects. GDPR compliance at 94% indicates that the framework has substantially incorporated data protection and privacy considerations, crucial for power systems that may handle consumer data. The framework's strengths in data protection, privacy by design, and breach notification align well with GDPR requirements. The identified area for improvement in cross-border data transfers is particularly relevant for utilities operating across multiple jurisdictions.

These compliance results suggest that the proposed framework provides a solid foundation for meeting regulatory requirements in the electric power sector. Its high alignment with multiple standards indicates its potential for wide applicability across different regulatory environments. This comprehensive sensitivity analysis not only enhances our understanding of the intricate dynamics within the algorithms but also provides actionable insights for practitioners aiming to deploy these algorithms in real-world scenarios. Future work could delve into further refinements and optimizations based on these nuanced findings.

4. Discussion

The framework demonstrated high effectiveness in threat detection and prevention, with rates exceeding 95% across various attack types. This level of protection represents a substantial improvement over traditional security measures and addresses the complex threat landscape unique to IoT-integrated power systems. The multi-layered approach proved particularly effective, with each layer contributing significantly to the overall security posture while maintaining acceptable performance overhead. The near-perfect device authentication rate (99.97%) and high detection of compromise attempts (98.9%) establish a robust first line of defense, crucial for maintaining

the integrity of vast IoT networks in power grids. This finding underscores the importance of device-level security in IoT environments, where each connected device represents a potential entry point for attackers. The communication layer's performance, particularly the low rate of successful man-in-the-middle attacks (0.07%), highlights the effectiveness of the implemented encryption and secure routing mechanisms. This is especially significant given the resource constraints of many IoT devices and the critical nature of power system communications [12].

The framework's scalability characteristics, demonstrating sub-linear increases in CPU utilization as the number of devices grew from 100 to 10,000, suggest its potential applicability in large-scale power systems. However, the linear growth in memory consumption indicates that further optimization may be necessary for very large-scale deployments. The framework's resilience, maintaining over 98% system availability during various attack scenarios, is particularly crucial for power systems where service continuity is paramount. These findings align with and extend previous research in the field. For instance, Wang et al. [21] proposed a multi-layer security architecture for smart grids, achieving a 92% detection rate for cyber-attack. Our framework's higher detection rates (96-99%) suggest that the integration of advanced machine learning techniques and blockchain technology has enhanced threat detection capabilities. Similarly, the scalability results compare favorably with those reported by Chen et al. [22], who observed performance degradation at around 5,000 IoT devices. Our framework's ability to maintain acceptable performance up to 10,000 devices represents a significant improvement.

However, our findings diverge from some previous studies in terms of the performance impact of security measures. Liu et al. [23] reported an average 15% increase in system latency when implementing comprehensive security measures in a simulated smart grid environment. In contrast, our framework introduced only a 2.3% increase in network latency at the 1,000-device scale, suggesting that our lightweight encryption algorithms and optimized network security measures are more efficient.

The high compliance levels with industry standards (94-98%) align with the findings of Vegesna [24], who emphasized the importance of standards alignment for practical implementation of cybersecurity frameworks in critical infrastructure. Our cost-benefit analysis reveals compelling economic implications for implementing this framework. Initial deployment costs range from $150-200 per IoT de-

vice, encompassing hardware security modules ($75-100), software licensing ($45-60), installation ($30-40), and training ($10-15). For a typical 1,000-device deployment, organizations can expect first-year investments of $500,000-750,000, with annual maintenance costs of $75,000-150,000 (15-20% of initial investment) covering security updates, audits, and training. Additional infrastructure requirements include network enhancements ($50,000-100,000), security monitoring ($75,000-150,000), and backup systems ($25,000-50,000). However, these investments are justified by substantial benefits: prevention of cyber incidents (saving $2.3M-4.5M per avoided major breach), reduced insurance premiums (15-25%), improved operational efficiency (8-12% reduction in downtime), and enhanced regulatory compliance. With the average cost of a major security breach in the power sector at $3.85M, organizations implementing this framework typically achieve ROI within 18-24 months through breach prevention and operational efficiencies.

5. Conclusions

The comprehensive evaluation of the proposed cybersecurity framework for IoT-integrated electric power information systems demonstrates its significant potential to enhance the security posture of modern power grids. The framework's multi-layered approach, combining advanced technologies such as machine learning and blockchain, proved highly effective in detecting and preventing a wide range of cyber threats. With detection rates exceeding 96% and prevention rates above 95% across various attack scenarios, the framework represents a substantial improvement over traditional security measures. Main strengths of the framework include its scalability, maintaining robust performance up to 10,000 IoT devices, and its resilience, ensuring high system availability even under attack conditions. The framework's compliance with major industry standards further underscores its practical applicability in real-world power systems. These findings suggest that the proposed solution effectively addresses the unique challenges posed by the integration of IoT devices in critical power infrastructure.

For organizations seeking to implement this framework, we recommend a structured three-phase approach spanning 9-13 months. The initial Assessment and Planning phase (2-3 months) focuses on conducting security audits, defining requirements, and establishing baseline metrics, with initial costs estimated at $150-200 per IoT device for hardware security modules and software licensing. This is followed by a Pilot Implementation phase (3-4 months) involving controlled deployment of core security measures including device authentication, encryption protocols, and anomaly detection systems in an environment of 100-500 devices. The final Scaled Deployment phase (4-6 months) encompasses full production rollout with advanced features such as machine learning-based threat detection and blockchain logging, establishing SOC procedures, with expected annual maintenance costs of 15-20% of initial implementation. Successful implementation requires several key factors including executive sponsorship, comprehensive documentation, clear incident response procedures, regular staff training, continuous monitoring, and compliance audits. Organizations must also ensure adequate resource allocation across technical expertise (cybersecurity specialists, network engineers, IoT specialists), infrastructure (security appliances, monitoring systems, backup facilities), software platforms (security management, analytics, logging systems), and training programs (staff certification, security awareness).

However, the study also revealed areas for further improvement and research. The linear growth in memory consumption at larger scales, the need for more extensive real-world testing, and the importance of addressing human factors in cybersecurity emerged as significant considerations for future work. Additionally, the rapidly evolving nature of cyber threats necessitates ongoing research to ensure the framework remains effective against emerging attack vectors. This study contributes valuable insights to the field of cybersecurity for IoT-integrated power systems. The proposed framework offers a promising foundation for enhancing the security of critical energy infrastructure in an increasingly connected world. With the provided implementation guidance, organizations can systematically adopt these security measures while addressing their specific operational needs. Future research directions, including real-world implementation studies, advanced threat modeling, and investigation of extreme scalability scenarios, will be crucial in further refining and validating this approach. As power systems continue to evolve and incorporate more IoT technologies, the development and implementation of robust, adaptable, and efficient cybersecurity solutions remains paramount to ensuring the reliability and resilience of our energy infrastructure.

Despite the promising results, this study has several limitations that should be considered. Firstly,

the simulated environment, while designed to closely mimic real-world conditions, may not capture all the complexities and variabilities of actual power grid operations. Real-world implementations may face unforeseen challenges do not present in the simulated environment. Secondly, the study focused on a specific set of attack scenarios and threat models. While these were chosen to represent common and significant threats, the rapidly evolving nature of cyber-attacks means that new, unforeseen attack vectors may emerge that were not considered in this study. Thirdly, the scalability testing was limited to 10,000 devices. While this covers the needs of many current power systems, future IoT deployments may significantly exceed this scale, potentially introducing new challenges not observed in our tests. Lastly, the study did not extensively explore the human factors in cybersecurity, such as user behavior and social engineering attacks. These aspects can significantly impact the overall security posture of a system and warrant further investigation. While our simulation attempted to recreate real-world conditions, certain network characteristics such as jitter, packet loss, and environmental interference could not be fully replicated in the laboratory setting. Additionally, while this study focused on framework performance in a controlled testbed environment, real-world deployments would need to consider the impact of geographic distribution on system performance. The effects of spatial distribution on latency, reliability, and security effectiveness across large distances represent an important area for future research.

Acknowledgment

Funding

References

[1] D. Anyanwu, "Cybersecurity in the age of internet of things: A review of challenges and solutions," Fac. Nat. Appl. Sci. J. Comput. Appl., vol. 1, no. 1, pp. 1–9, 2024.

[2] E. James and F. Rabbi, "Fortifying the IoT landscape: Strategies to counter security risks in connected systems," Tensorgate J. Sustain. Technol. Infrastruct. Dev. Ctries., vol. 6, no. 1, pp. 32–46, 2023.

[3] J. Vostoupal and K. Uhlířová, "Of Hackers and Privateers: The Possible Evolution of the Problem of Cyber-Attribution," Masaryk Univ. J. Law Technol., vol. 18, no. 2, pp. 169–214, 2024, doi: 10.5817/mujlt2024-2-2.

[4] T. Johansmeyer, "How Reversibility Differentiates Cyber from Kinetic Warfare: A Case Study in the Energy Sector," Int. J. Secur. Privacy Trust Manag., vol. 12, no. 1, pp. 1–14, 2023, doi: 10.5121/ijsptm.2023.12101.

[5] S. A. Hashmi, C. F. Ali, and S. Zafar, "Internet of things and cloud computing-based energy management system for demand side management in smart grid," Int. J. Energy Res., vol. 45, no. 1, pp. 1007–1022, 2021, doi: 10.1002/er.6141.

[6] B. G. Kang and B. S. Kim, "Attachable IoT-based digital twin framework specialized for SME production lines," Int. J. Simul. Model., vol. 23, no. 3, pp. 471–482, Sep. 2024, doi: 10.2507/IJSIMM23-3-694.

[7] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," IEEE Syst. J., vol. 17, no. 4, pp. 6695–6709, 2023, doi: 10.1109/JSYST.2023.3305757.

[8] A. Rekeraho, D. T. Cotfas, P. A. Cotfas, T. C. Bălan, E. Tuyishime, and R. Acheampong, "Cybersecurity challenges in IoT-based smart renewable energy," Int. J. Inf. Secur., vol. 23, no. 1, pp. 101–117, 2024, doi: 10.1007/s10207-023-00732-9.

[9] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," J. Supercomput, vol. 76, no. 7, pp. 5320–5363, 2020, doi: 10.1007/s11227-019-02945-z.

[10] R. Karthikeyani and E. Karthikeyan, "A Review on Distributed Denial of Service Attack," Asian J. Res. Comput. Sci., vol. 16, no. 4, pp. 133–144, 2023, doi: 10.9734/AJRCOS/2023/v16i4378.

[11] K. Vaigandla, N. Azmi, and R. Karne, "Investigation on intrusion detection systems (IDSs) in IoT," Int. J. Emerg. Trends Eng. Res., vol. 10, no. 3, 2022, doi: 10.30534/ijeter/2022/041032022.

[12] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," J. Netw. Comput. Appl., vol. 209, p. 103540, 2023, doi: 10.1016/j.jnca.2022.103540 .

[13] R. J. Rabelo, S. P. Zambiasi, and D. Romero, "Softbots 4.0: supporting cyber-physical social systems in smart production management," Int. J. Ind. Eng. Manag., vol. 14, no. 1, pp. 63–93, 2023, doi: 10.24867/IJIEM-2023-1-325.

[14] J. Basulo-Ribeiro, M. Amorim, and L. Teixeira, "How to accelerate digital transformation in companies with Lean Philosophy? Contributions based on a practical case," Int. J. Ind. Eng. Manag., vol. 14, no. 2, pp. 94–104, 2023, doi: 10.24867/IJIEM-2023-2-326.

[15] S. Zahoor and R. N. Mir, "Resource management in pervasive Internet of Things: A survey," J. King Saud Univ.-Comput. Inf. Sci., vol. 33, no. 8, pp. 921–935, 2021, doi: 10.1016/j.jksuci.2018.08.014.

[16] F. E. Salamh, U. Karabiyik, and M. Rogers, "A constructive direst security threat modeling for drone as a service," J. Digit. Forensics Secur. Law, vol. 16, no. 1, p. 2, 2021, doi: 10.15394/jdfsl.2021.1695.

[17] E. Süren, F. Heiding, J. Olegård, and R. Lagerström, "PatrIoT: practical and agile threat research for IoT," Int. J. Inf. Secur., vol. 22, no. 1, pp. 213–233, 2023, doi: 10.1007/s10207-022-00633-3.

[18] F. Thabit, S. A.-H. Alhomdy, A. Alahdal, and S. B. Jagtap, "Exploration of security challenges in cloud computing: Issues, threats, and attacks with their alleviating techniques," J. Inf. Comput. Sci., vol. 12, no. 10, pp. 17-41, 2020.

[19] H. Jahangir, S. Lakshminarayana, C. Maple, and G. Epiphaniou, "A Deep-Learning-Based Solution for Securing the Power Grid Against Load Altering Threats by IoT-Enabled Devices," IEEE Internet Things J., vol. 10, no. 12, pp. 10687-10697, 2023, doi: 10.1109/JIOT.2023.3240289.

[20] D. Mukherjee et al., "Cyber Security: Perspective of Challenges in Operational Technology Systems in Power Sector," Power Res.-J. CPRI, pp. 35–45, 2024, doi: 10.33686/pwj.v20i1.1168.

[21] Y. Wang, T.-L. Nguyen, Y. Xu, Q.-T. Tran, and R. Caire, "Peer-to-peer control for networked microgrids: Multi-layer and multi-agent architecture design," IEEE Trans. Smart Grid, vol. 11, no. 6, pp. 4688–4699, 2020, doi: 10.1109/TSG.2020.3006883.

[22] L. Chen, W. Hu, K. Jamieson, X. Chen, D. Fang, and J. Gummeson, "Pushing the physical limits of IoT devices with programmable metasurfaces," in Proc. 18th USENIX Symp. Netw. Syst. Design Implement. (NSDI 21), 2021, pp. 425–438.

[23] M. Liu et al., "Enhancing Cyber-Resiliency of DER-Based Smart Grid: A Survey," IEEE Trans. Smart Grid, vol. 15, no. 5, pp. 4998-5030, 2024, doi: 10.1109/TSG.2024.3373008

[24] V. V. Vegesna, "Cybersecurity of Critical Infrastructure," Int. Mach. Learn. J. Comput. Eng., vol. 7, no. 7, pp. 1–17, 2024.