SPECTRUM OF ENGINEERING SCIENCES
ISSN (E) 3007-3138 (P) 3007-312X VOLUME 4, ISSUE 6, 2026

ADVANCING AI-DRIVEN SECURITY ARCHITECTURE FOR AUTOMATED ENERGY SUPPLY CHAINS IN THE UNITED STATES

Sadia Ali Watara[*1], **Zeliatu Ahmed**[2]

[*1]*Department of Information Systems, Dakota State University, USA*
[2]*Department of Information Systems, University of Maryland, Baltimore County, USA*

[*1]sadia.Watara@trojans.dsu.edu, [2]ahmedzeliya@gmail.com

DOI: https://doi.org/10.5281/zenodo.20591283

Keywords
artificial intelligence; cybersecurity; smart grid; automated energy supply chain; SCADA security; machine learning intrusion detection; federated learning; blockchain; critical infrastructure protection; adversarial AI; NERC CIP; IoT security

Article History
Received: 08 April 2026
Accepted: 20 May 2026
Published: 08 June 2026

Corresponding Author: *
Sadia Ali Watara

Abstract

The modernization of United States energy infrastructure through artificial intelligence (AI), Industrial Internet of Things (IIoT), smart grids, cloud-integrated energy management systems, autonomous monitoring platforms, and digitally interconnected supply chain networks has significantly improved operational efficiency, predictive maintenance, and real-time decision-making across power generation, transmission, and distribution environments. However, the rapid digitalization of automated energy supply chains has simultaneously expanded the cyberattack surface, exposing critical infrastructure to increasingly sophisticated threats including ransomware, adversarial AI attacks, supply chain compromise, SCADA manipulation, insider threats, and large-scale data exfiltration. Energy systems now process enormous volumes of operational technology (OT), information technology (IT), and consumer energy usage data across interconnected cyber-physical ecosystems, making security resilience a national priority for the United States. This article presents a comprehensive analysis of AI-driven security architectures for protecting automated energy supply chains in the United States. The study evaluates machine learning-based intrusion detection systems, federated learning security frameworks, blockchain-enabled energy data governance, deep learning anomaly detection, and adversarial defense mechanisms for critical energy infrastructure. Threats are analyzed across five interconnected system layers including physical infrastructure, industrial control systems, communication networks, cloud analytics, and AI decision-making platforms. The article further examines alignment with U.S. regulatory frameworks including NIST Cybersecurity Framework 2.0, NERC CIP standards, Executive Order 14028, DOE cybersecurity guidelines, and CISA critical infrastructure directives. A multi-phase implementation roadmap is proposed to guide U.S. energy operators toward resilient, privacy-preserving, and AI-enhanced cybersecurity ecosystems. The analysis demonstrates that layered AI-driven architectures integrating federated learning, blockchain provenance, zero-trust networking, and adversarial robust deep learning models provide the most effective defense strategy for securing next-generation automated energy supply chains in the United States.

1. Introduction

The United States energy sector is experiencing a profound digital transformation driven by the integration of artificial intelligence, Industrial Internet of Things, cloud computing, edge analytics, smart grid technologies, autonomous

monitoring systems, and advanced energy management platforms. Electric utilities, renewable energy providers, oil and gas distribution networks, and national transmission operators increasingly depend on automated cyber-physical infrastructures capable of real-time sensing, predictive maintenance, adaptive load balancing, and intelligent operational optimization.

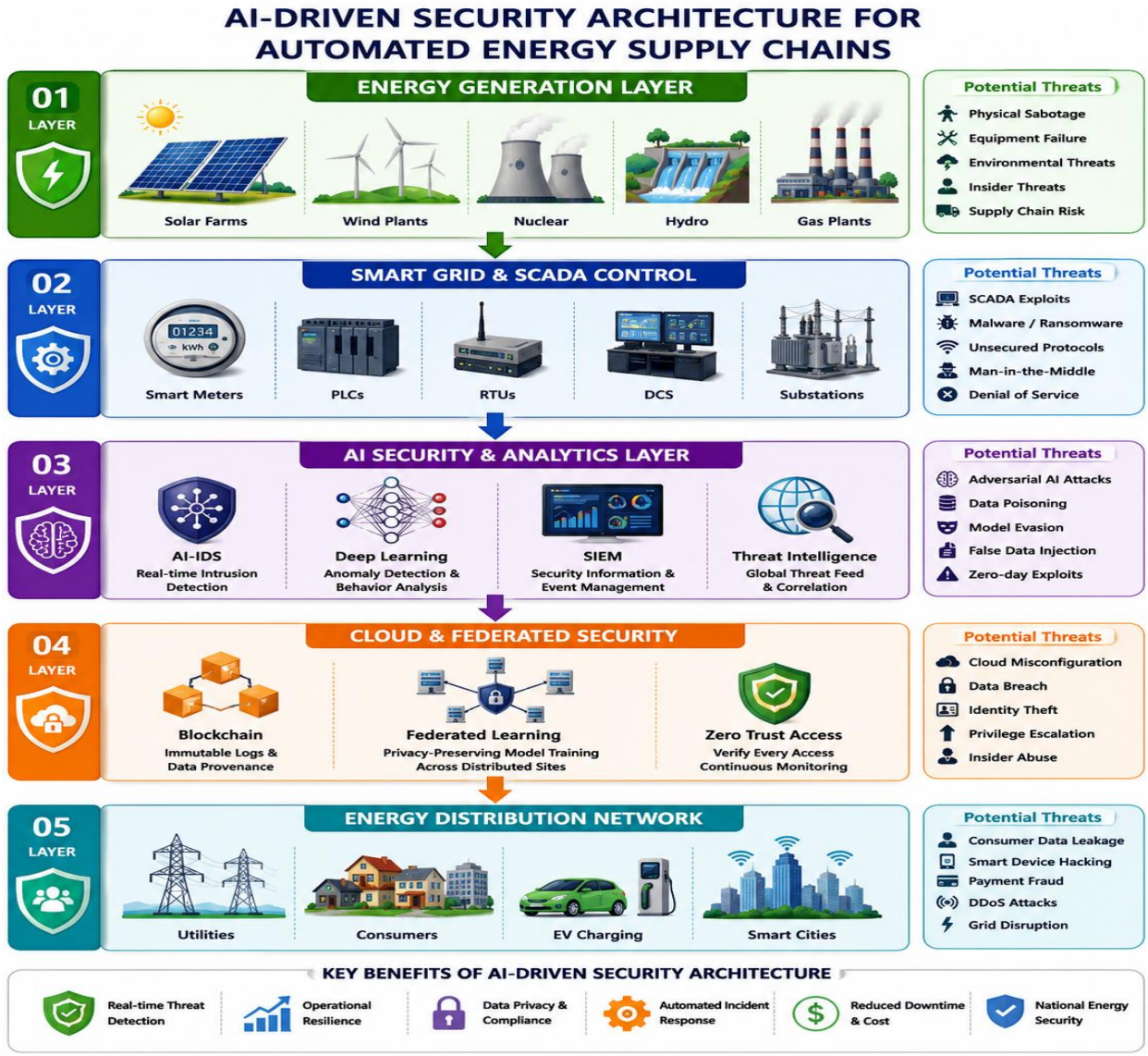
Modern automated energy supply chains encompass interconnected systems responsible for electricity generation, transmission, storage, and distribution across geographically dispersed infrastructures. Smart substations, AI-enabled grid management platforms, intelligent metering systems, automated demand-response frameworks, and autonomous industrial control systems continuously exchange large volumes of operational and consumer data through highly interconnected networks.

The convergence of operational technology (OT) and information technology (IT) environments has significantly expanded the attack surface of U.S. critical energy infrastructure. Historically isolated industrial control systems such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and programmable logic controllers (PLCs) are now increasingly connected to enterprise networks, cloud platforms, and third-party vendor ecosystems. Artificial intelligence has emerged as a critical technology for defending modern energy infrastructures against sophisticated cyber threats. AI-driven intrusion detection systems, anomaly detection frameworks, behavioral analytics platforms, and predictive threat intelligence systems provide adaptive, scalable, and real-time security capabilities that significantly outperform traditional signature-based defenses.

Furthermore, the growing adoption of renewable energy systems, autonomous grid management, and AI-enabled industrial automation has intensified the need for resilient and intelligent cybersecurity frameworks capable of defending against rapidly evolving cyber threats. Traditional rule-based security mechanisms are no longer sufficient for protecting highly dynamic and interconnected energy ecosystems where attackers increasingly utilize sophisticated techniques such as AI-powered malware, ransomware campaigns, adversarial machine learning, and supply chain infiltration. Therefore, the integration of advanced AI-driven security architectures combining deep learning, federated intelligence, blockchain governance, and zero trust principles has become essential for ensuring operational continuity, infrastructure reliability, data integrity, and national energy security within the United States.

In conclusion, the rapid evolution of artificial intelligence, smart grids, Industrial Internet of Things, and cloud-based automation technologies has fundamentally transformed the cybersecurity requirements of modern energy supply chains in the United States. As cyber threats targeting critical infrastructure continue to grow in sophistication, traditional security mechanisms are becoming insufficient for protecting interconnected energy ecosystems. Therefore, the adoption of AI-driven, multilayered, and resilient cybersecurity architectures integrating deep learning, federated intelligence, blockchain governance, and zero trust principles is essential for ensuring operational continuity, infrastructure reliability, data privacy, and national energy security. This study highlights the importance of intelligent, adaptive, and future-ready defense frameworks capable of safeguarding next-generation automated energy infrastructures against evolving cyber risks and emerging digital threats. Overall, the integration of AI-driven cybersecurity technologies has become essential for protecting modern automated energy supply chains from evolving cyber threats. By combining intelligent threat detection, secure data governance, and adaptive defense mechanisms, energy infrastructures can achieve greater resilience, reliability, and operational security in highly interconnected digital environments.

Figure 1: AI-Driven Security Architecture for Automated Energy Supply Chain



2. Background and Related Work

2.1 Artificial Intelligence in Energy Infrastructure Security

Artificial intelligence technologies have become increasingly important in protecting critical infrastructure environments due to their ability to process massive volumes of heterogeneous operational data in real time [1]. AI systems deployed in energy environments support anomaly detection, predictive maintenance, cyber threat intelligence, asset monitoring, demand forecasting, and automated response orchestration [2,3].

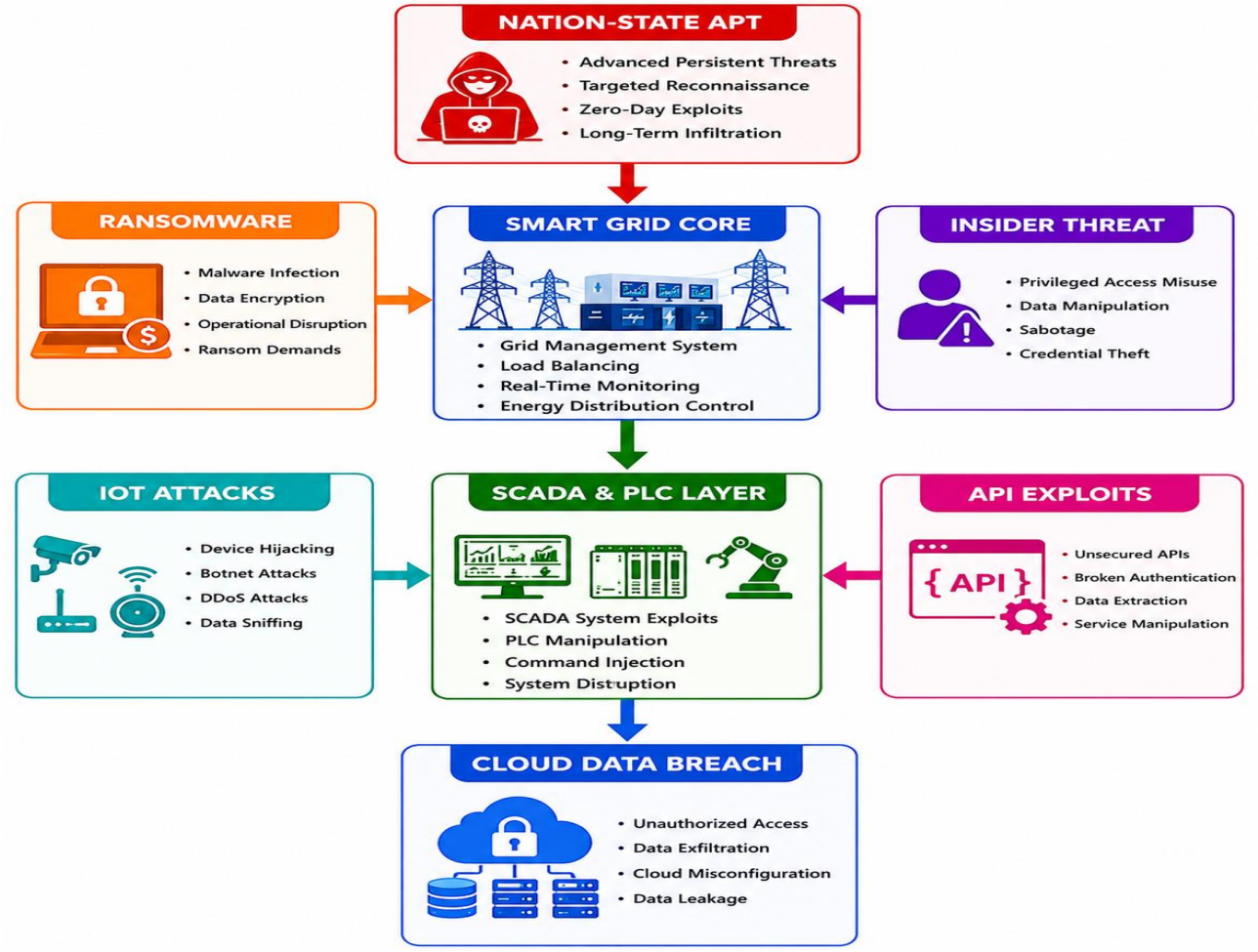
Machine learning techniques such as Random Forest, Support Vector Machines (SVM), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Deep Reinforcement Learning (DRL) have demonstrated substantial effectiveness in detecting abnormal operational behaviors within smart grids and industrial control environments [4,5].

2.2 Smart Grid and SCADA Security

Smart grids represent one of the most critical components of modern energy infrastructures [6]. These systems integrate advanced metering infrastructure (AMI), renewable energy management systems, intelligent substations, distributed control mechanisms, and IoT-

enabled monitoring frameworks to optimize electricity generation and distribution [7,8]. However, smart grid environments remain highly vulnerable to cyberattacks due to legacy infrastructure components, insecure communication protocols, insufficient encryption mechanisms, and growing interconnectivity between operational and enterprise networks [9,10].

Figure 2: Smart Grid Cybersecurity Threat Landscape



2.3 Industrial Internet of Things (IIoT) Security in Energy Systems

The Industrial Internet of Things has become a fundamental component of modern energy infrastructures by enabling real-time monitoring, intelligent automation, predictive maintenance, and remote operational control [11]. Smart sensors, connected meters, industrial gateways, and edge devices continuously exchange operational data across interconnected energy networks [12]. However, the increasing deployment of the Industrial Internet of Things devices introduces significant cybersecurity risks due to insecure communication protocols, limited device-level security, weak authentication mechanisms, and inadequate firmware protection [13,14]. Attackers can exploit vulnerable the Industrial Internet of Things devices to launch distributed denial-of-service attacks, unauthorized system access, and data manipulation campaigns [15]. Therefore, secure the Industrial Internet of Things architectures integrated with AI-driven monitoring and anomaly detection systems are essential for protecting smart energy environments [16].

2.4 Cloud Computing and Edge Intelligence in Energy Security

Cloud computing and edge intelligence technologies play an increasingly important role in supporting automated energy supply chains by enabling scalable data storage, real-time analytics, and intelligent decision-making [17, 18]. Cloud-based energy management systems allow centralized monitoring of geographically distributed infrastructures, while edge computing improves response speed by processing critical operational data closer to industrial devices and control systems [19]. Despite these advantages, cloud-integrated infrastructures remain vulnerable to cybersecurity threats such as unauthorized access, API exploitation, credential theft, and data breaches [20]. Additionally, insecure edge devices can serve as entry points for attackers targeting critical infrastructure systems [21]. Consequently, secure cloud governance, AI-driven access control, and encrypted edge communication frameworks are necessary for maintaining operational security and resilience [22].

2.5 Blockchain Applications in Energy Cybersecurity

Blockchain technology has emerged as a promising solution for improving cybersecurity, transparency, and trust within modern energy ecosystems [23]. Decentralized ledger systems provide immutable and tamper-resistant records for operational activities, energy transactions, and device authentication processes [24]. Blockchain-based frameworks can enhance supply chain traceability, support secure peer-to-peer energy trading, and improve data integrity across interconnected infrastructures [25]. Smart contracts further automate security enforcement and operational verification processes within distributed energy networks. However, blockchain implementation also introduces challenges related to scalability, computational overhead, transaction latency, and integration complexity [26]. Despite these limitations, blockchain governance remains a valuable component of resilient AI-driven cybersecurity architectures [27].

2.6 AI-Based Threat Intelligence and Predictive Security

Artificial intelligence has significantly improved modern cybersecurity operations through intelligent threat intelligence, predictive analytics, and automated incident response capabilities [28]. AI-driven security systems analyze large volumes of operational and network data to identify suspicious patterns, emerging attack behaviors, and potential vulnerabilities before they cause operational disruption [29]. Predictive security models utilizing machine learning algorithms can forecast cyber risks, prioritize threat mitigation strategies, and support proactive defense mechanisms in smart grid and industrial control environments [30]. Furthermore, AI-enabled Security Information and Event Management (SIEM) platforms enhance security operations by automating threat correlation and incident analysis. These capabilities strengthen cyber resilience across automated energy infrastructures [31].

2.7 Zero Trust Security for Critical Energy Infrastructure

Zero Trust Architecture (ZTA) has become an important cybersecurity strategy for protecting critical energy infrastructures against increasingly sophisticated cyber threats [32]. Unlike traditional perimeter-based security models, zero trust frameworks operate on the principle of continuous verification, where every user, device, application, and communication request must be authenticated before access is granted [33]. This approach minimizes insider threats, unauthorized lateral movement, and credential-based attacks within interconnected energy environments [34]. Micro-segmentation, behavioral analytics, multi-factor authentication, and least-privilege access control further strengthen system security and operational resilience. As energy infrastructures continue to adopt cloud computing, IIoT devices, and remote operations, zero trust networking provides a robust foundation for securing modern cyber-physical ecosystems [35].

3. Threat Landscape in Automated Energy Supply Chains

3.1 Energy Infrastructure Attack Surface

Modern automated energy supply chains operate through multiple interconnected technological layers that collectively support energy generation, transmission, monitoring, control, and distribution processes. These infrastructures begin with the physical infrastructure layer, which includes smart meters, substations, transformers, renewable energy plants, and industrial sensors responsible for real-time operational monitoring and energy production. Above this layer exists the industrial control and SCADA layer, where Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), programmable logic controllers (PLCs), and remote terminal units (RTUs) manage critical industrial operations and automated decision execution. The communication and networking layer facilitates continuous data exchange between devices, control centers, cloud platforms, and operational networks through IoT gateways, wireless communication protocols, 5G connectivity, and enterprise network infrastructures. Furthermore, the cloud and analytics layer provide centralized data storage, predictive analytics, real-time monitoring dashboards, and AI-driven energy management services using cloud computing and big data technologies. Finally, the AI and autonomous decision-making layer integrates advanced machine learning algorithms, deep learning models, intelligent automation systems, and predictive cybersecurity frameworks capable of autonomously detecting anomalies, optimizing energy distribution, forecasting demand fluctuations, and responding to emerging cyber threats. The high level of interconnectivity among these layers significantly enhances operational efficiency and automation capabilities; however, it simultaneously expands the cybersecurity attack surface, making modern energy infrastructures increasingly vulnerable to sophisticated cyberattacks and operational disruptions.

Table 1: Energy Supply Chain Security Layers and Vulnerabilities

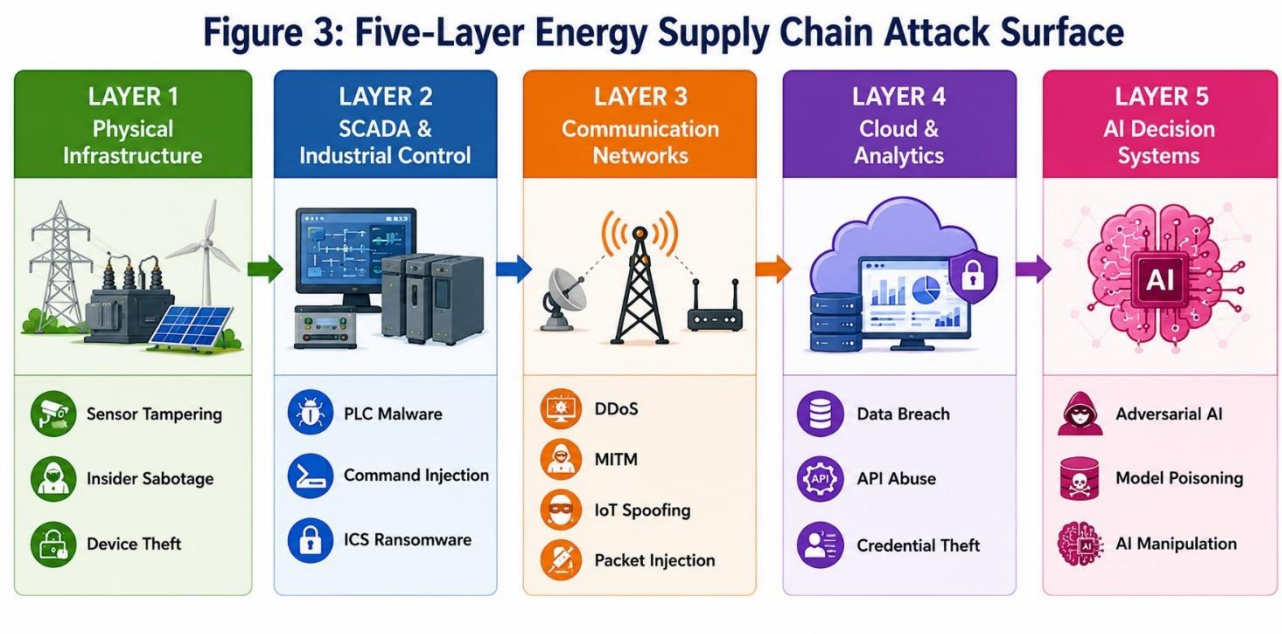
System Layer	Technology Component	Security Vulnerability	Attack Vector	Regulatory Exposure
Physical Infrastructure	Smart meters, transformers, substations	Physical tampering, sensor manipulation	Insider attacks, sabotage	NERC CIP
SCADA / ICS	PLCs, DCS, SCADA servers	Command injection, malware infection	ICS malware, ransomware	DOE, CISA
Network Communication	IoT gateways, 5G, AMI networks	Traffic interception, spoofing	MITM, DDoS	NIST SP 800-53
Cloud Analytics	Cloud energy management systems	Data exfiltration, credential theft	API exploitation	CCPA
AI Decision Systems	Deep learning security platforms	Adversarial attacks, model poisoning	AI evasion attacks	Executive Order 14028

3.2 Five-Layer Cybersecurity Attack Surface in Automated Energy Supply Chains

The Five-Layer Energy Supply Chain Attack Surface model illustrates the complex and interconnected cybersecurity risks associated with modern automated energy infrastructures. At the foundation lies the Physical Infrastructure Layer, which includes smart meters, substations, transformers, industrial sensors, and energy generation equipment that remain vulnerable to threats such as sensor tampering, insider sabotage, and physical device theft. Above this is the SCADA and Industrial Control Layer, where programmable logic controllers, distributed control systems, and SCADA platforms manage critical industrial operations and face threats including PLC malware infections, command injection attacks, and industrial ransomware targeting operational technology environments. The Communication

Networks Layer enables data transmission across IoT devices, wireless gateways, enterprise systems, and cloud-connected infrastructures; however, this layer is highly susceptible to distributed denial-of-service attacks, man-in-the-middle attacks, IoT spoofing, and malicious packet injection. The Cloud and Analytics Layer supports centralized monitoring, predictive analytics, and real-time energy management services but introduces vulnerabilities related to cloud data breaches, API exploitation, and credential theft. Finally, the AI Decision Systems Layer represents the most advanced operational tier where artificial intelligence and autonomous decision-making systems perform threat detection, predictive maintenance, and energy optimization. Despite their advanced capabilities, these AI-driven systems remain vulnerable to adversarial AI attacks, model poisoning, and AI manipulation attempts capable of compromising automated decision-making processes. Collectively, these five interconnected layers demonstrate the expanding cybersecurity attack surface of modern energy supply chains and emphasize the urgent need for multilayered AI-driven defense architectures capable of protecting critical infrastructure environments against sophisticated cyber threats.

Figure 3: Five-Layer Energy Supply Chain Attack Surface



4. AI-Driven Security Architecture

4.1 Layered AI Security Framework

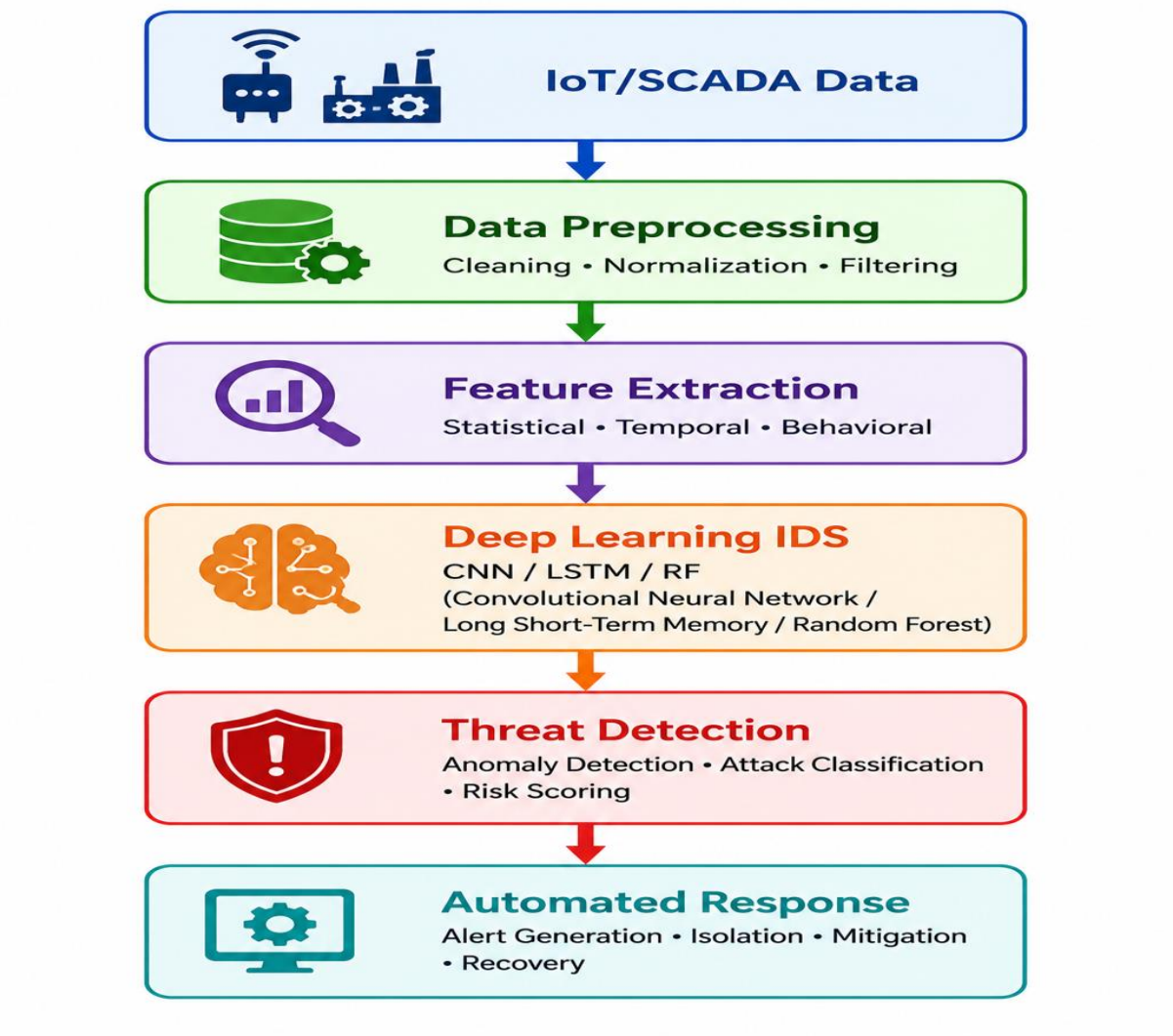
The proposed AI-driven security architecture integrates multiple defensive technologies across all operational layers of the energy supply chain.

Core Components:

The proposed AI-driven security architecture incorporates several advanced core components designed to enhance the cybersecurity resilience of automated energy supply chains. AI-powered Intrusion Detection Systems (IDS) continuously monitor network traffic, operational activities, and system behaviors to identify malicious activities and unauthorized access attempts in real time. Behavioral Analytics Engines analyze user behavior, device interactions, and operational patterns to detect abnormal activities that may indicate insider threats, compromise systems, or cyberattacks. Federated Learning Security Models enable collaborative threat intelligence and distributed AI training across multiple energy infrastructures without exposing sensitive operational data, thereby improving privacy preservation and regulatory compliance. Blockchain-Based Data Governance mechanisms provide secure, immutable, and tamper-resistant records for operational logs, device authentication, and energy transactions, ensuring transparency and data integrity throughout the supply chain.

Additionally, Zero Trust Architecture (ZTA) enforces continuous verification, strict authentication policies, and least-privilege access controls across all connected devices, users, and systems. Threat Intelligence Correlation Systems further strengthen security by aggregating and analyzing threat data from multiple internal and external sources to identify emerging attack patterns and coordinated cyber threats. Finally, Automated Incident Response Platforms enable rapid detection, containment, mitigation, and recovery from cyber incidents through intelligent automation and AI-driven response orchestration, significantly reducing operational downtime and improving overall infrastructure resilience.

Figure 4: AI-Based Intrusion Detection Pipeline



4.2 Deep Learning Intrusion Detection Systems

Deep learning IDS frameworks leverage CNNs, LSTMs, and Autoencoders to detect cyberattacks in energy environments.

Advantages:

The proposed AI-driven intrusion detection framework offers several significant advantages for securing automated energy supply chains and critical infrastructure environments. One of the primary benefits is real-time threat detection, which enables continuous monitoring of network traffic, SCADA communications, and IoT device activities to rapidly identify malicious behavior and cyber intrusions before they cause operational disruption. The architecture also provides adaptive learning capability through advanced machine learning and deep learning algorithms that continuously improve detection

performance by learning from evolving attack patterns and operational behaviors. Furthermore, the system achieves high anomaly detection accuracy by utilizing intelligent models such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and Random Forest classifiers capable of recognizing both known and previously unseen cyber threats. Another major advantage is the reduction of false positive rates, which minimizes unnecessary alerts and improves the efficiency of security operations centers by focusing attention on genuine security incidents. Additionally, the framework supports behavioral pattern recognition, allowing the system to analyze user activities, device interactions, and operational sequences to detect insider threats, abnormal behaviors, and sophisticated attack techniques that traditional signature-based systems may fail to identify. Together, these capabilities significantly enhance the resilience, reliability, and cybersecurity posture of modern AI-driven energy infrastructures.

Table 2: AI Models for Energy Infrastructure Security

AI Model	Security Function	Application Area	Performance
CNN	Intrusion Detection	Smart Grid Traffic	High Accuracy
LSTM	Sequential Anomaly Detection	SCADA Monitoring	Real-Time Detection
Random Forest	Threat Classification	IoT Device Security	Fast Processing
Autoencoder	Anomaly Detection	Energy Analytics	Low False Positives
Federated Learning	Collaborative Threat Detection	Multi-Site Infrastructure	Privacy Preserving

5. Federated Learning and Blockchain Security

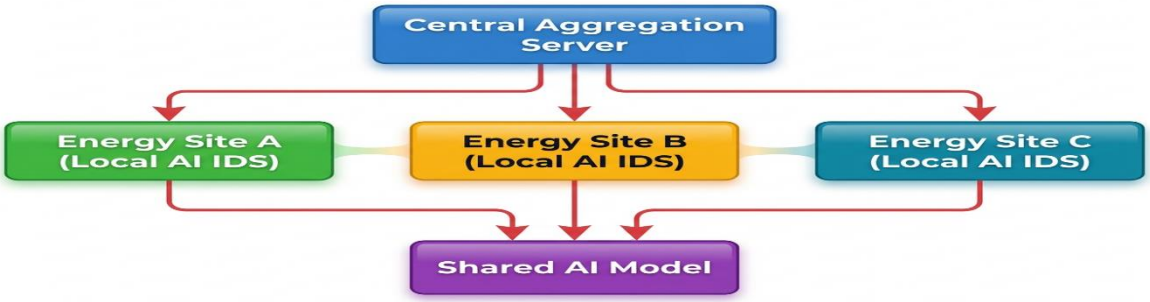
5.1 Federated Security Intelligence

Federated learning enables collaborative cybersecurity intelligence across geographically distributed energy infrastructures while preserving operational data privacy.

Benefits:

The federated learning-based security framework provides several important benefits for protecting automated energy supply chains and critical infrastructure environments. One of its primary advantages is the elimination of centralized raw data exposure, as sensitive operational and cybersecurity data remain within local energy facilities rather than being transferred to a central server. This decentralized learning approach significantly strengthens data protection and minimizes the risk of large-scale information leakage. Additionally, federated learning improves regulatory compliance by supporting privacy-preserving AI training methods that align with cybersecurity and data governance standards such as NIST, CISA, and critical infrastructure protection guidelines. The framework also enables cross-organization threat intelligence sharing, allowing multiple energy operators, utilities, and infrastructure providers to collaboratively improve AI security models by exchanging learned model parameters instead of sensitive operational data. Furthermore, the architecture reduces privacy risks by ensuring that confidential industrial information, consumer energy usage patterns, and SCADA operational data remain securely stored within local environments. Another major advantage is enhanced resilience against data breaches, as attackers cannot easily access a centralized repository containing critical infrastructure data. Collectively, these benefits make federated learning a highly effective and scalable solution for securing modern AI-driven energy ecosystems while maintaining operational privacy, collaboration, and regulatory compliance.

Figure 5: Federated Learning Security Architecture



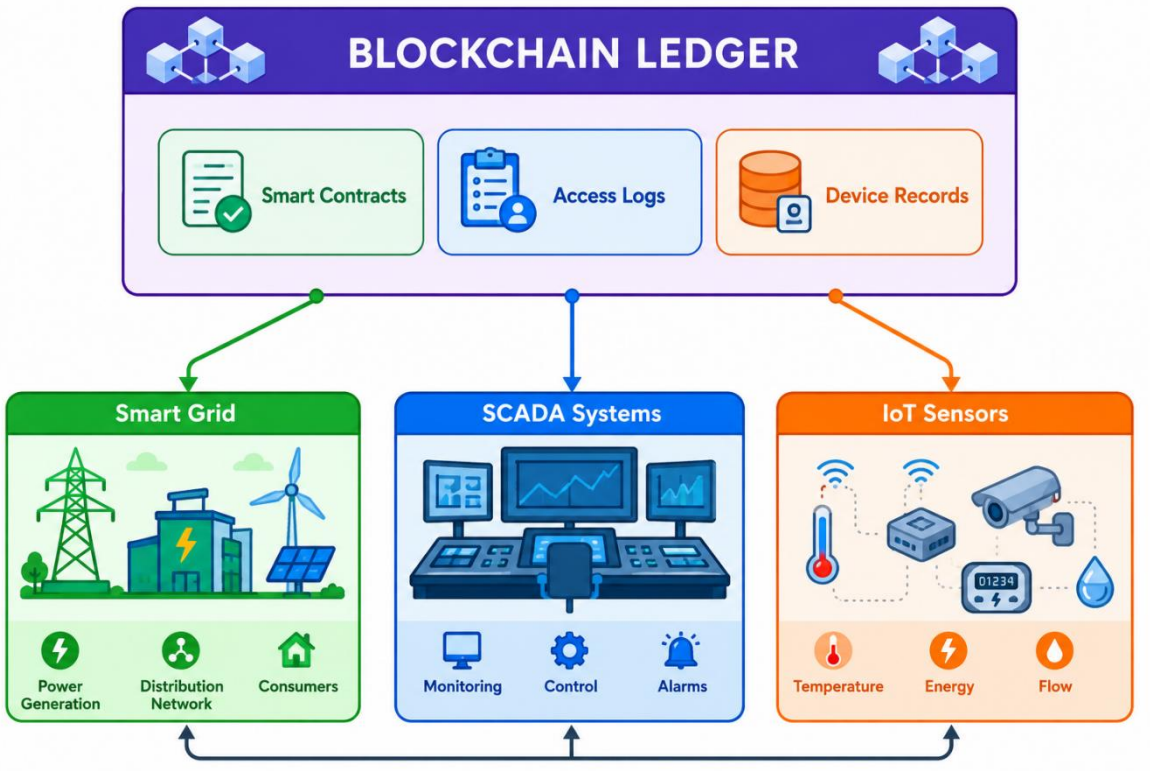
5.2 Blockchain-Based Governance

Blockchain technologies provide immutable audit trails for operational activities across energy supply chains.

Applications:

The proposed framework supports several practical applications in modern smart energy and IoT environments. It enables secure energy transaction logging by storing energy exchange records in an immutable and decentralized manner, ensuring transparency and preventing unauthorized modifications. Device identity verification is achieved through blockchain-based authentication mechanisms that validate the legitimacy of connected devices before communication or data exchange. The system also provides tamper-resistant telemetry by securely recording sensor and operational data, protecting it from alteration or cyber manipulation. In addition, smart contract enforcement automates predefined operational rules and agreements, reducing human intervention and improving system efficiency. Furthermore, the framework supports supply chain provenance tracking by maintaining a transparent history of product movement and operational events, which enhances traceability, accountability, and trust across the entire supply chain network.

Figure 6: Blockchain-Secured Energy Governance Framework



6. Adversarial Attacks and Defense Mechanisms

6.1 Adversarial Machine Learning Threats

AI security systems are vulnerable to adversarial attacks designed to manipulate model behavior.

Major Threat Categories:

Machine learning and AI-based systems in smart environments face several major cybersecurity threat categories that can compromise their reliability and performance. Evasion attacks occur when attackers manipulate input data to deceive the AI model into making incorrect predictions or classifications during operation. Model poisoning attacks target the training phase by injecting malicious or misleading data into the dataset, causing the model to learn incorrect patterns. Data manipulation involves altering or corrupting system data, which can affect decision-making accuracy and reduce system integrity. Model inversion attacks attempt to reconstruct sensitive training information from the model outputs, posing serious privacy and confidentiality risks. Backdoor attacks introduce hidden triggers into the model during training, allowing attackers to force malicious behavior whenever specific conditions or inputs are activated.

Figure 7: Adversarial Attack Taxonomy in Energy AI Systems

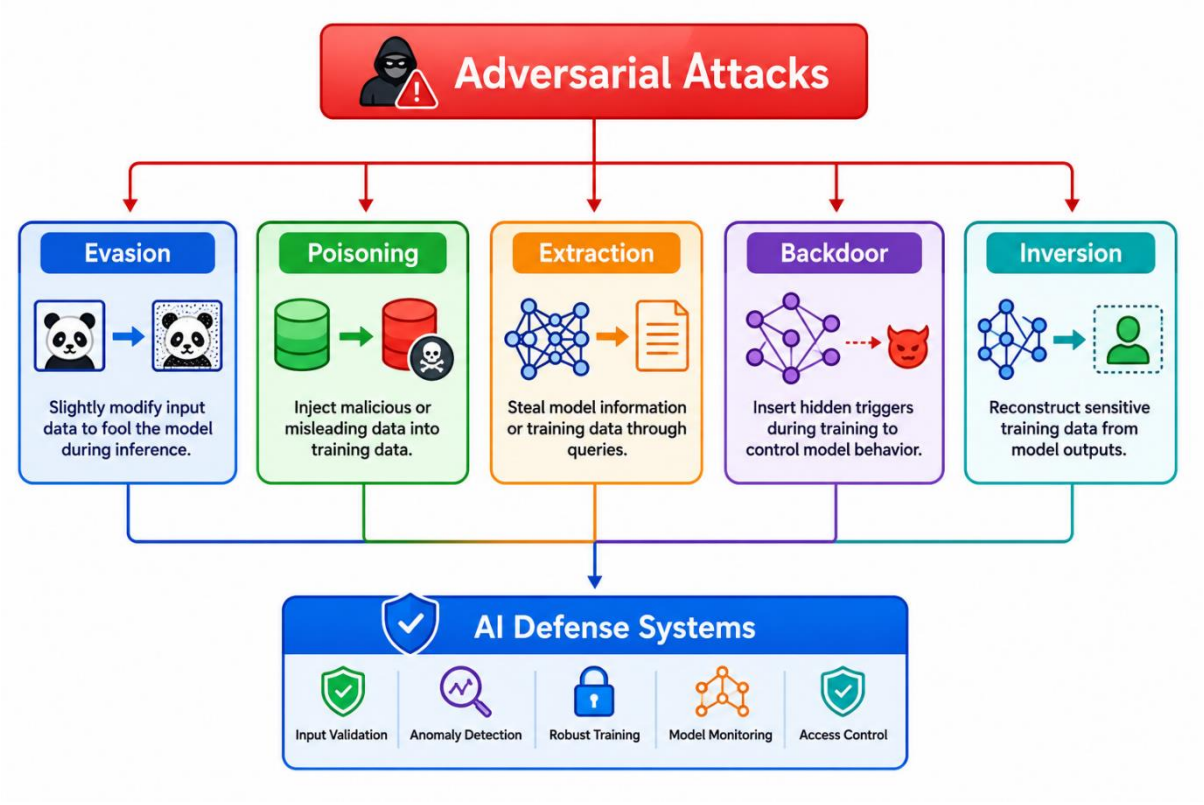


Table 3: Adversarial Attacks and Defense Mechanisms

Attack Type	Target	Defense Mechanism
Evasion Attack	IDS Models	Adversarial Training
Model Poisoning	Federated Learning	Byzantine Aggregation
Model Extraction	AI APIs	Differential Privacy
Backdoor Attack	Deep Learning Models	Explainable AI Auditing
Data Exfiltration	IoT Sensors	Blockchain Provenance

7. Zero Trust Architecture for Energy Security

7.1 Zero Trust Security Model

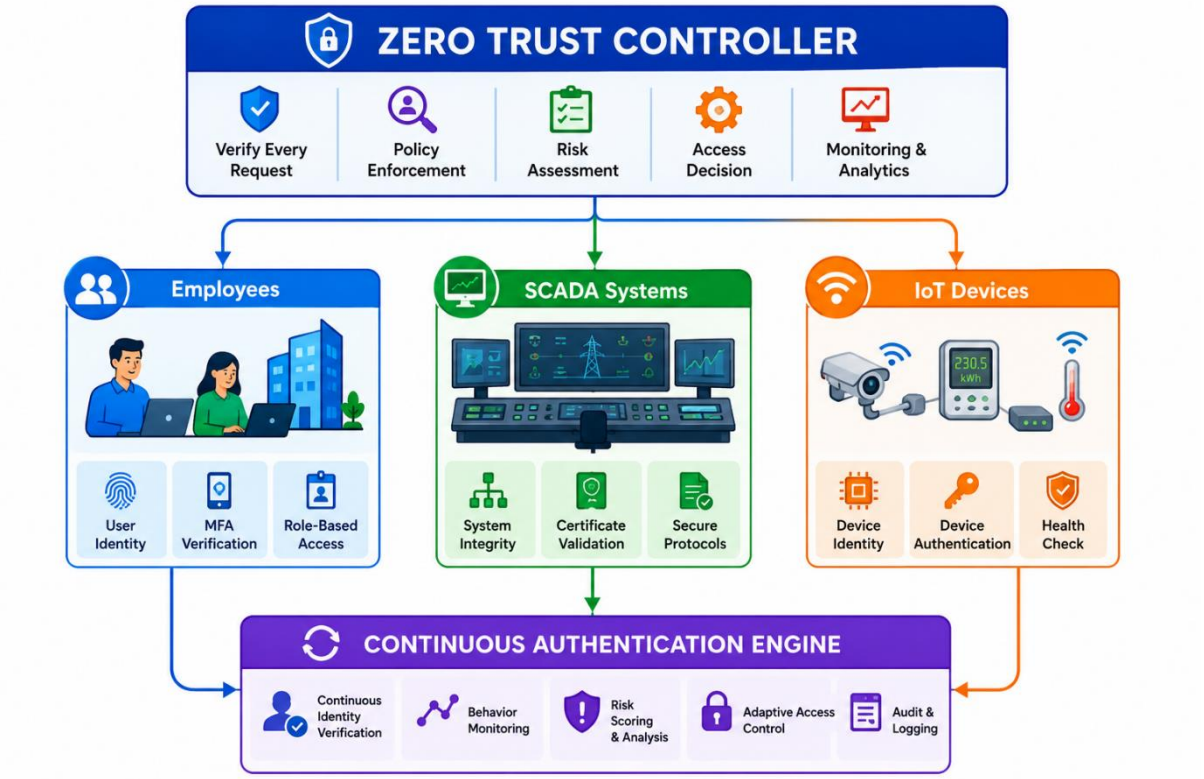
Zero Trust principles enforce continuous authentication and least-privilege access

controls across all energy infrastructure components.

Key Principles:

The Zero Trust Security Model is based on several core principles designed to strengthen the protection of modern energy infrastructure systems. The principle of "Never trust, always verify" ensures that every user, device, and application must be authenticated before accessing network resources, regardless of whether they are inside or outside the system boundary. Continuous authentication further enhances security by constantly validating user identities and device integrity throughout the communication session rather than relying on a single login event. Micro-segmentation divides the network into smaller isolated segments, limiting unauthorized lateral movement and reducing the impact of potential cyberattacks. Least privilege access restricts users and devices to only the minimum permissions required to perform their tasks, minimizing security risks caused by excessive access rights. Additionally, behavioral risk scoring continuously monitors user and device activities to detect abnormal behavior patterns and dynamically adjust security responses based on the assessed risk level.

Figure 8: Zero Trust Energy Security Architecture



8. Regulatory and Compliance Framework

8.1 NERC CIP Standards

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) framework establishes mandatory cybersecurity requirements for bulk electric systems.

Major Requirements:

The NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) standards establish mandatory cybersecurity requirements to ensure the protection of bulk electric systems from cyber threats and operational risks. These standards include strict access control measures to ensure that only authorized personnel can access critical infrastructure systems. They also require timely incident reporting to ensure that any cybersecurity breach or suspicious activity is documented and communicated for rapid response and mitigation. Asset management is another key requirement, focusing on maintaining an accurate inventory of all critical

cyber assets to ensure proper protection and oversight. Vulnerability assessment is used to regularly identify, evaluate, and address security weaknesses within the system before they can be exploited. In addition, continuous security monitoring is implemented to detect anomalies, track system behavior, and ensure ongoing compliance with cybersecurity policies and standards.

8.2 NIST Cybersecurity Framework 2.0

The NIST CSF provides five core security functions:

The NIST Cybersecurity Framework (CSF) is built around five core security functions that provide a structured approach to managing and reducing cybersecurity risks. The first function, Identify, focuses on understanding and managing cybersecurity risks related to systems, assets, data, and capabilities. The second function, Protect, involves implementing safeguards such as access controls, encryption, and security training to ensure critical infrastructure and services are secured. The third function, Detect, emphasizes the continuous monitoring of systems to identify cybersecurity events and anomalies in a timely manner. The fourth function, Respond, involves taking appropriate actions to contain and mitigate the impact of detected incidents, including incident response planning and communication. Finally, the Recover function focuses on restoring and maintaining normal operations after a cybersecurity incident, ensuring system resilience and continuous improvement based on lessons learned.

Figure 9: NIST Cybersecurity Framework Integration

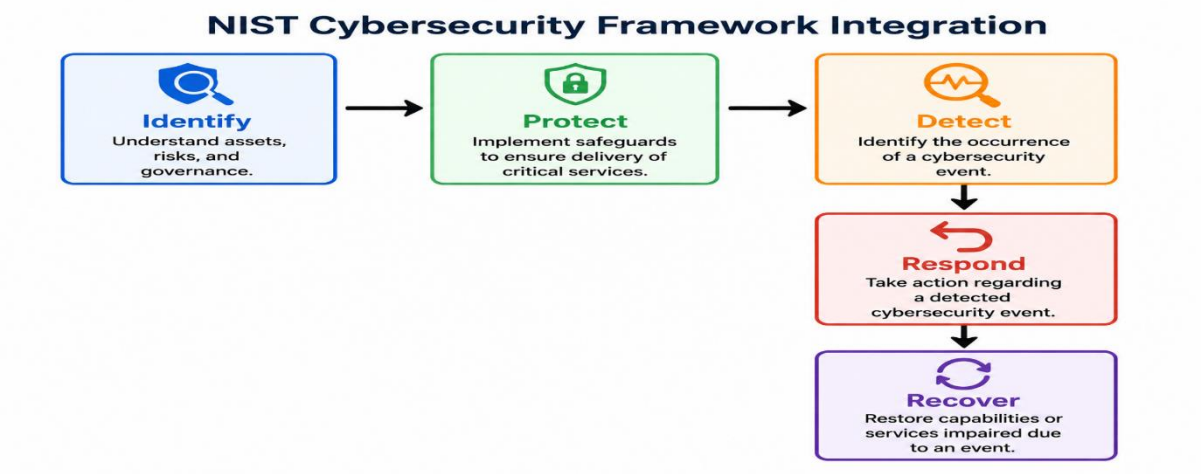
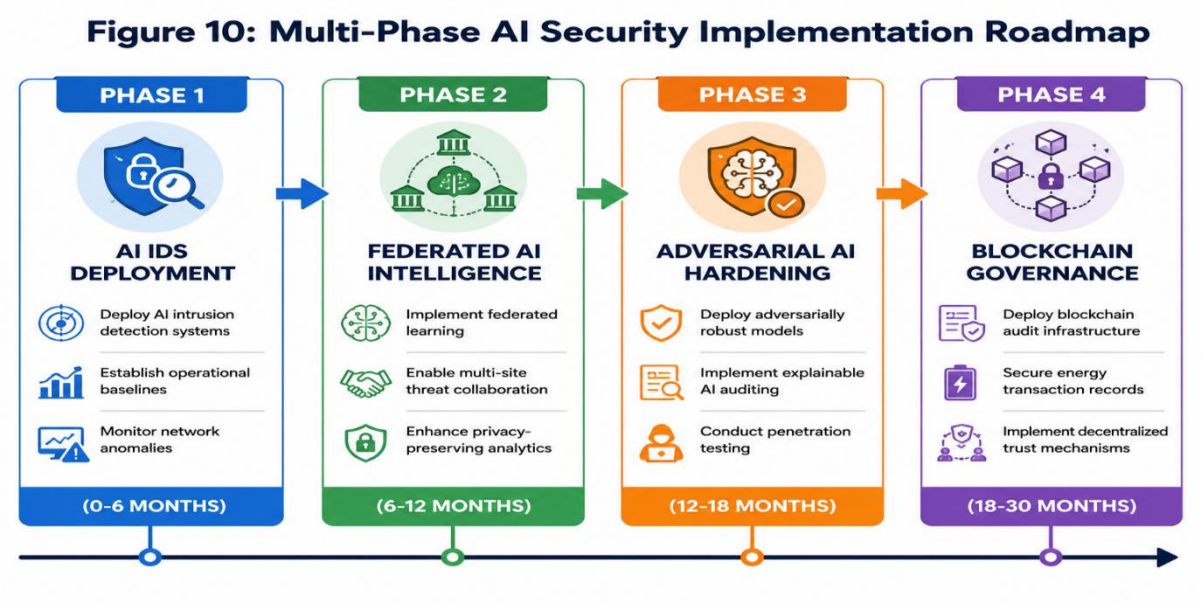


Table 4: U.S. Regulatory Alignment for AI Security

Regulation	Security Objective	AI Alignment
NERC CIP	Critical Infrastructure Protection	AI-IDS Monitoring
NIST CSF 2.0	Cybersecurity Governance	Threat Detection
Executive Order 14028	National Cybersecurity	Zero Trust & AI
DOE C2M2	Energy Security Maturity	AI Risk Analytics
CISA Directives	Incident Response	Automated Threat Intelligence

9. Implementation Roadmap

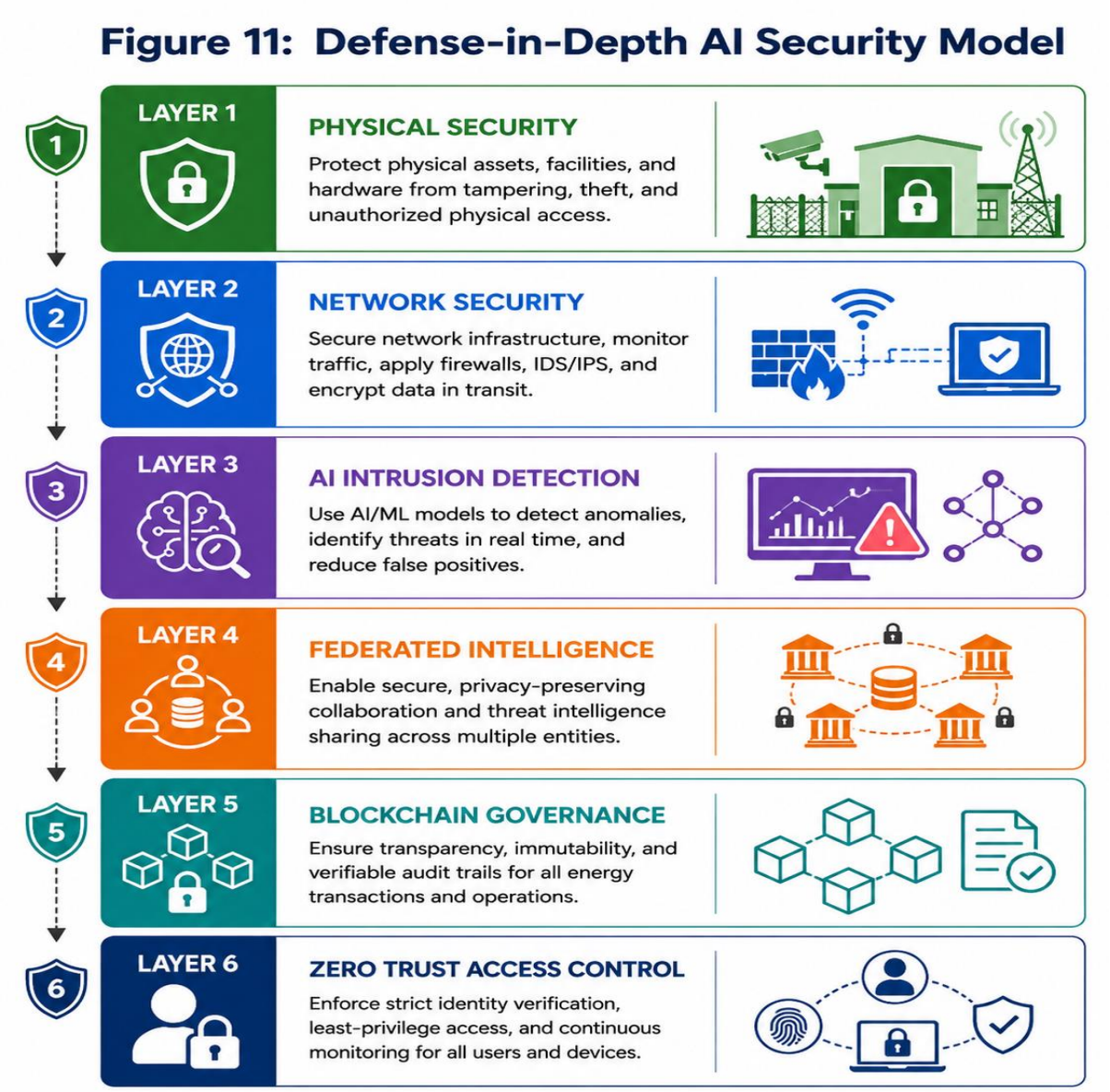
Figure 10: Multi-Phase AI Security Implementation Roadmap



9.5 Defense-in-Depth AI Security Model – Conceptual Overview

A defense-in-depth AI security model is essential for protecting automated energy supply chains against increasingly sophisticated cyber threats. This multi-layered approach ensures that if one security layer is compromised, additional protective mechanisms remain in place to detect, prevent, and mitigate potential attacks. The model begins with physical security to protect critical infrastructure and hardware assets from unauthorized access and physical tampering. Network security further strengthens the system by securing communication channels, monitoring traffic, and preventing external intrusions. AI-based intrusion detection enhances real-time threat monitoring by identifying suspicious activities and abnormal behavior patterns, while federated intelligence enables secure collaboration among distributed entities without compromising sensitive data privacy. Additionally, blockchain governance improves transparency and trust through tamper-resistant audit records, and zero trust access control ensures continuous identity verification and strict access management. Together, these interconnected layers create a resilient, adaptive, and comprehensive cybersecurity framework for modern energy infrastructures.

Figure 11: Defense-in-Depth AI Security Model



10. Discussion

The findings of this study demonstrate that AI-driven security architectures significantly improve cyber resilience across automated energy supply chains. With the increasing adoption of smart grids, Industrial Internet of Things (IIoT) devices, and intelligent energy management systems, cybersecurity threats have become more complex and difficult to manage using traditional rule-based approaches. AI-powered cybersecurity systems provide adaptive and predictive capabilities that improve threat detection, incident response, and operational continuity. However, the analysis also indicates that no single AI framework can fully address all cybersecurity requirements, as each technology introduces both advantages and limitations. Deep learning-based Intrusion Detection Systems (IDS) show strong effectiveness in detecting cyber threats, network anomalies, and malicious activities with high accuracy. These systems can identify sophisticated attack patterns and support proactive security monitoring across energy infrastructures. Nevertheless, deep learning models remain vulnerable to adversarial attacks, where manipulated inputs can mislead AI systems and reduce detection reliability. Additionally, federated learning improves privacy preservation by enabling collaborative AI model training without directly sharing sensitive operational data, although challenges such as model

aggregation complexity, communication overhead, and coordination difficulties may affect implementation effectiveness.

Blockchain technology further strengthens cybersecurity governance by improving transparency, accountability, and tamper-resistant auditing of energy transactions and operational records. Decentralized trust mechanisms reduce dependence on centralized authorities and improve system integrity across interconnected energy networks. However, blockchain adoption introduces scalability concerns, including increased computational requirements, transaction delays, and integration challenges with existing infrastructure. Similarly, zero trust networking enhances security by continuously verifying users and devices, thereby reducing unauthorized access risks within smart energy ecosystems.

Overall, the findings suggest that a defense-in-depth cybersecurity strategy provides the most effective protection for U.S. energy infrastructures. A layered framework integrating AI anomaly detection, federated learning, blockchain governance, zero trust networking, and adversarial hardening creates a more resilient security posture against evolving cyber threats. Furthermore, explainable AI auditing and continuous penetration testing are essential to ensure transparency, accountability, and long-term reliability of intelligent cybersecurity systems. Such an integrated approach can significantly strengthen the security and sustainability of future automated energy supply chains.

11. Limitations and Challenges

One of the major limitations of AI-driven cybersecurity architectures in automated energy supply chains is the high computational and infrastructure cost associated with deploying advanced machine learning and deep learning models. Technologies such as CNNs, LSTMs, federated learning, and blockchain require significant processing power, high-performance storage systems, and continuous network connectivity. Many legacy energy infrastructures in the United States still operate on outdated hardware and industrial control systems that may not fully support modern AI-based security frameworks. Additionally, the integration of cloud computing, real-time analytics, and edge intelligence increases operational expenses and maintenance complexity for energy operators.

Although artificial intelligence improves threat detection capabilities, AI systems themselves remain vulnerable to adversarial cyberattacks. Attackers can manipulate input data, poison training datasets, or exploit weaknesses in machine learning models to bypass intrusion detection systems and influence automated decision-making processes. Adversarial AI attacks, model inversion, backdoor attacks, and AI evasion techniques can reduce the reliability and accuracy of cybersecurity systems operating within smart grids and SCADA environments. Furthermore, the increasing use of AI-powered malware and automated attack tools creates additional security challenges for protecting critical energy infrastructures.

Modern energy ecosystems generate massive volumes of operational, consumer, and industrial data across interconnected cyber-physical systems. Sharing cybersecurity intelligence among multiple organizations while preserving privacy remains a significant challenge. Although federated learning reduces centralized data exposure, issues related to communication overhead, synchronization, interoperability, and regulatory compliance still exist. Energy operators must also comply with multiple regulatory frameworks such as NERC CIP, NIST CSF 2.0, DOE guidelines, and CISA directives, which can complicate implementation and governance processes across distributed infrastructures.

Another important challenge is the complexity of integrating AI-driven security architectures with existing legacy infrastructure, industrial control systems, and heterogeneous communication technologies. Energy environments consist of diverse hardware, proprietary protocols, IoT devices, cloud platforms, and SCADA systems that often lack standardization and interoperability. Moreover, blockchain-based governance mechanisms may introduce scalability limitations such as transaction delays, increased energy consumption, and storage overhead. Maintaining real-time performance, low latency, and continuous monitoring across

geographically distributed energy supply chains therefore remains a difficult task for large-scale deployments.

12. Conclusion

The digital transformation of U.S. energy infrastructures has created unprecedented opportunities for operational intelligence, automation, and efficiency while simultaneously expanding the cyberattack surface of critical national infrastructure. Automated energy supply chains now depend heavily on interconnected AI-driven cyber-physical systems that require adaptive, scalable, and resilient security architectures capable of defending against increasingly sophisticated cyber threats.

This study presented a comprehensive analysis of AI-driven security architectures for automated energy supply chains in the United States. The article examined the evolving threat landscape, evaluated deep learning intrusion detection systems, explored federated privacy-preserving intelligence frameworks, analyzed adversarial attack scenarios, and proposed blockchain-supported governance mechanisms aligned with national cybersecurity objectives.

The findings demonstrate that layered AI-driven cybersecurity ecosystems integrating deep learning IDS, federated learning, blockchain provenance, zero trust architecture, and adversarially robust AI models provide the strongest defense against emerging threats targeting smart grids, SCADA systems, and automated energy infrastructures.

REFERENCES

Khalaf, Noora Zidan, et al. "Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure." *Mesopotamian Journal of CyberSecurity* 5.2 (2025): 501-513.

Iyaniwura, Abdulrahman Adebola, and Charles Sunday Mayaki. "Artificial Intelligence-enabled smart grid systems for real-time load forecasting, fault detection, renewable energy integration and optimization." *Global Journal of Engineering and Technology Advances* 24.03 (2025): 191-208.

Jamil, Muhammad, et al. "Collection and Identification of Tick Species on Goats and Sheep in Dera Ismail Khan, Pakistan." *Annals of the Romanian Society for Cell Biology* 25.6 (2021).

Afzal, Saira, et al. "Machine Learning Analysis Empowered Evaluation of English Learning Apps for User Level." *Spectrum of Engineering Sciences* (2025): 1836-1851.

Delshadi, Amirmohammad, et al. "ARTIFICIAL INTELLIGENCE FOR STRENGTHENING CYBERSECURITY IN EDUCATIONAL TECHNOLOGY SYSTEMS." *Spectrum of Engineering Sciences* 4.3 (2026): 299-311.

Akram, Muhammad, et al. "CYBERSECURITY RISK ASSESSMENT MODEL FOR INTERNET OF MEDICAL THINGS (IOMT) DEVICES IN HEALTHCARE SYSTEMS." *Spectrum of Engineering Sciences* 4.3 (2026): 312-326.

Safiullah, Dilshad, et al. "Integrating Artificial Intelligence and Soil Ecology to Enhance Plant Resilience under Environmental Stress." *ASSAJ* 4.02 (2025): 3508-3516.

Nazir, Muhammad Ashraf, et al. "The Silent Guard: ML-Based Zero-Knowledge Proofs in Blockchain Security." *Spectrum of Engineering Sciences* (2025): 1659-1678.

Delshadi, Amir Mohammad, et al. "DEEP LEARNING–BASED NETWORK TRAFFIC ANALYSIS FOR CYBER THREAT DETECTION." *Spectrum of Engineering Sciences* 3.12 (2025): 607-614.

Iqbal, Muhammad Waleed, et al. "MITIGATING DDOS ATTACKS ON IOT DEVICES: A HYBRID APPROACH USING AI AND BLOCKCHAIN." *Spectrum of Engineering Sciences* (2025): 1679-1697.

Rasheed, Muhammad Danish, et al. "LEVERAGING ARTIFICIAL INTELLIGENCE FOR ADVANCE DATA NETWORKING AND CYBERSECURITY." *Spectrum of Engineering Sciences* 4.3 (2026): 286-298.

Zeeshan, Muhammad, et al. "MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR STRENGTHENING CYBER SECURITY IN INTRUSION DETECTION SYSTEM." *Spectrum of Engineering Sciences* (2025): 1274-1286.

Hasanat, Syed Muhammad, et al. "Enhancing load forecasting accuracy in smart grids: a novel parallel multichannel network approach using 1D CNN and Bi-LSTM models." *International Journal of Energy Research* 2024.1 (2024): 2403847.

Rahman, Shoaib Ur, et al. "Failures and Repairs: An Examination of Software System Failure." *Bulletin of Business and Economics (BBE)* 13.1 (2024).

Watara, Sadia Ali, Gerardo Moreira, and Vincent Anyah. "Enhancing Supply Chain Efficiency Through Machine Learning: A Predictive Analytics Approach to Risk Identification and Timely Deliveries." (2025).

Hamid, Khalid, et al. "Topological Evaluation of Cloud Computing Networks and Real-Time Scenario-Based Effective Usage." *Bulletin of Business and Economics (BBE)* 13.2 (2024): 80-92.

Arshid, Noman, et al. "An Innovative Framework for Automated Software Testing and Validation." *Bulletin of Business and Economics (BBE)* 13.1 (2024).

Ahmed, Rana Hassam, Majid Hussain, and Ashraf Khalil. "Blockchain-based supply chain management in healthcare." *AI and Blockchain Applications for Privacy and Security in Smart Medical Systems*. IGI Global Scientific Publishing, 2025. 107-132.

Ahmed, Rana Hassam, et al. "Enhancing autonomous vehicle security through advanced artificial intelligence techniques." *Journal of Computer Science and Electrical Engineering* 6.4 (2024): 1-6.

Ahmed, Rana Hassam, et al. "Integrating Large Language Models and AI into Blockchain: A Framework for Intelligent Smart Contracts and Fraud Detection." *IEEE Access* (2025).

Hanif, Mehran, et al. "Evaluating Prompt Variability in Transformer-Based LLMs Through Discrete and Semantic PSI." *ASSAJ* 4.02 (2025): 1798-1809.

Zia, Khadija, et al. "ADVANCED MACHINE LEARNING FRAMEWORK FOR IDENTIFYING AND MITIGATING FAKE NEWS AND MISINFORMATION PROPAGATION ON SOCIAL MEDIA PLATFORMS." *Spectrum of Engineering Sciences* (2025): 142-154.

Hamid, Khalid, et al. "ML-based Meta-Model Usability Evaluation of Mobile Medical Apps." *International Journal of Advanced Computer Science & Applications* 15.1 (2024).

Iqbal, Muhammad Waseem, et al. "Meta-analysis and investigation of usability attributes for evaluating operating systems." *Migration Letters* 21.5 (2024): 1363-1380.

Riaz, Samavia, et al. "Software Development Empowered and Secured by Integrating A DevSecOps Design." *Journal of Computing & Biomedical Informatics* 8.02 (2025).

Khaliq, Khowla, et al. "Ransomware Attacks: Tools and Techniques for Detection." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

Malik, Naeem Akhtar, et al. "Behavior and Characteristics of Ransomware-A Survey." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

Delshadi, Amir Mohammad, et al. "Empowerment of Artificial Intelligence (AI) in preventing and detecting ransomware: an analytical review." *Spectrum of Engineering Sciences* (2025): 36-48.

Ibrar, Muhammad, et al. "Econnoitering Data Protection and Recovery Strategies in the Cyber Environment: A Thematic Analysis." *International Journal for Electronic Crime Investigation* 8 (2024).

Iqbal, Muhammad Waleed, et al. "TOWARDS NEXT-GENERATION AUTOMATION: DATA-DRIVEN SYNERGIES OF AI AND ROBOTICS THROUGH DATA ENGINEERING AND DATA SCIENCE." *Spectrum of Engineering Sciences* (2025): 181-209.

Fahad, Muhammad, et al. "Embedding Artificial Intelligence in Games NPC and effects on emotional health." *Spectrum of Engineering Sciences* (2025): 1032-1042.

Usman, Yasir, et al. "Visually Impaired People Empowered by Deploying CNN-Based System on Low-Power Wearable Platforms." *Journal of Computing & Biomedical Informatics* (2025).

Campbell, Ruth, Mairéad MacSweeney, and Dafydd Waters. "Sign language and the brain: a review." *Journal of deaf studies and deaf education* 13.1 (2008): 3-20.

Alnaim, Abdulrahman K., and Ahmed M. Alwakeel. "Zero trust strategies for cyber-physical systems in 6G networks." *Mathematics* 13.7 (2025): 1108.