International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Designing a zero-trust cybersecurity architecture for smart grid communication systems to safeguard critical energy infrastructure

Ozioko Chidiebube Nelson [1,*], Emmanuel Ayodeji Osoko [2] and Temitope Ologunbaba [3]

[1] *Department of Computer and Information Systems, Prairie View A&M University, Texas, United States.*
[2] *Department of Electrical Engineering and Computer Science, Ohio University, Ohio, United States.*
[3] *Department of Electrical and Electronics Engineering, Federal University of Technology, Akure, Nigeria.*

International Journal of Science and Research Archive, 2023, 10(02), 1335-1348

Publication history: Received on 04 November 2023; revised on 20 December 2023; accepted on 24 December 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.10.2.1061

Abstract

The modernization of electricity grids through cloud computing has introduced unprecedented efficiency, scalability, and resilience to power delivery. However, it has also exposed critical infrastructure to new cyber threats. Nowhere is this duality more evident than in California, where utilities such as Southern California Edison (SCE) and regional operators like the California Independent System Operator (CAISO) are integrating cloud-native systems into smart grid operations. As these platforms interface with distributed energy resources, IoT-enabled metering, and edge analytics, traditional perimeter-based cybersecurity models are proving insufficient. This study proposes a Zero-Trust Penetration Architecture tailored for cloud-enabled smart grids, using California's energy infrastructure as a case example. The architecture incorporates identity-aware micro-segmentation, policy-based access controls, encrypted telemetry, and continuous authentication across cloud-OT boundaries. Through simulated attack scenarios involving ICS honeypots, cloud API vulnerability modeling, and telemetry breach analysis, the study quantifies improvements in breach containment, lateral threat resistance, and policy enforcement efficacy. Results demonstrate that zero-trust frameworks significantly reduce dwell time and unauthorized access spread in grid systems. The findings underscore the need for utilities—particularly those operating in high-risk, high-integration regions like California—to adopt ZTA-compliant security models in line with NIST 800-207 and evolving NERC-CIP standards.

Keywords: Zero Trust Architecture; Cloud Security; Smart Grid; California Energy Infrastructure; Southern California Edison; CAISO; NERC-CIP; Federated Identity

1. Introduction

The integration of cloud computing into smart electricity grids has revolutionized the energy sector across the United States. In particular, California—home to nearly 40 million residents and one of the most complex electricity infrastructures in the world—has emerged as a leader in grid modernization, digital energy management, and cloud adoption in utility operations (California Energy Commission, 2023). Utilities such as Southern California Edison (SCE), operating within the oversight of the California Independent System Operator (CAISO), now manage a vast array of distributed energy resources (DERs), electric vehicle chargers, demand response platforms, and IoT-based metering systems. These digital assets are increasingly controlled via cloud-native platforms for real-time analytics, predictive maintenance, and grid balancing.

However, this transition has also introduced serious vulnerabilities. The cyber-physical nature of smart grids—linking generation, transmission, distribution, and consumption through networked devices—has expanded the attack surface of critical infrastructure. As recent U.S. incidents have shown, adversaries exploit everything from legacy protocols (e.g.,

* Corresponding author: Ozioko Chidiebube Nelson

Copyright © 2023 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

Modbus/TCP) to exposed cloud APIs. The 2021 Colonial Pipeline ransomware attack and multiple breaches of municipal utilities in Texas, Florida, and California have reinforced the urgent need for advanced, adaptive security strategies across state-regulated and investor-owned utility systems (Cybersecurity & Infrastructure Security Agency [CISA], 2022).

Traditional perimeter-based models of cybersecurity—dependent on firewalls and static credentialing—are no longer effective in defending cloud-integrated energy systems. These models rely on implicit trust once users or devices are inside the network. Yet, cloud-based grid environments like those managed by SCE increasingly span public and private networks, contractor-managed systems, and third-party platforms such as AWS IoT Core, Azure Sphere, or Siemens' Grid Edge suite. Consequently, insider threats, lateral movement by adversaries, and insufficient identity verification have become prominent risks (NIST, 2022; DOE, 2023).

To address this, the Zero Trust Architecture (ZTA) model has gained traction in both federal and enterprise sectors. ZTA, first conceptualized by Kindervag (2010) and formally adopted into NIST Special Publication 800-207 (2020), advocates for the elimination of implicit trust and the implementation of continuous authentication, micro-segmentation, real-time telemetry, and strict access control. While ZTA is well-suited for enterprise IT systems, its structured deployment in cloud-integrated smart grids—especially within operational technology (OT) environments—remains limited. In California, for example, many substations and DER controls are still reliant on legacy SCADA systems that lack the protocol stack for ZTA compliance (Liu et al., 2022).

This study proposes a Zero-Trust Penetration Architecture for smart electricity grids, demonstrated through a detailed case study of SCE's digital grid platforms and CAISO's regional coordination protocols. The proposed system combines policy-based access brokering, identity-aware telemetry, and breach-resilient micro-segmentation to fortify cloud-linked grid systems. By simulating attack scenarios using ICS honeypots, penetration testing of cloud-device APIs, and telemetry breach logs, this study evaluates the impact of zero-trust mechanisms on breach detection times, lateral movement resistance, and access path validation.

Focusing on California as a high-risk, high-complexity zone with a mix of renewable integration, wildfire threats, and grid decentralization, this research offers a grounded framework for integrating zero-trust into the digital nervous system of U.S. power utilities. The study is aligned with evolving NERC-CIP compliance updates, federal Zero Trust mandates, and California's regulatory innovation goals in grid security.

2. Purpose and Specific Aims

This study seeks to address the escalating vulnerabilities of cloud-integrated smart electricity grids in the United States by proposing and evaluating a robust Zero-Trust Penetration Architecture (ZTPA). With the increasing digitization of grid control systems and the proliferation of distributed energy resources (DERs), the conventional trust-based network perimeter is rapidly becoming obsolete. Nowhere is this challenge more urgent than in California, where utilities such as Southern California Edison (SCE), operating under the regional governance of the California Independent System Operator (CAISO), have embraced cloud-native platforms to manage critical infrastructure functions ranging from grid stabilization to customer analytics.

The primary goal of this research is to design a scalable zero-trust framework specifically tailored for utility-driven, cloud-managed power systems, with emphasis on practical feasibility, security enhancement, and regulatory compliance. The architecture emphasizes identity-aware segmentation, continuous verification, dynamic policy enforcement, and encrypted telemetry to protect operational technology (OT) layers interconnected with cloud-based control interfaces. Drawing on the operational realities of SCE's infrastructure, the study will analyze typical vulnerabilities—including API exposure, credential misuse, and unauthorized lateral movement—through simulated attack environments such as ICS honeypots and telemetry-integrated breach simulations.

Beyond architectural design, the study aims to empirically assess the effectiveness of ZTPA in mitigating threats across various grid layers. Performance will be evaluated in terms of breach detection latency, access containment, privilege escalation resistance, and recovery response time. These metrics will be benchmarked against conventional perimeter-based security configurations, with a focus on operational environments reflective of U.S. investor-owned utilities (IOUs) and their compliance obligations under the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) standards.

In addition, the study is designed to generate practical recommendations for security practitioners and policymakers, aligning the proposed model with national cybersecurity directives such as NIST Special Publication 800-207 and recent

federal mandates for Zero Trust implementation across critical infrastructure sectors. Special attention is given to the broader applicability of the architecture for other U.S. regions, especially those integrating renewable energy at scale or operating in climate-sensitive zones such as wildfire-prone or high-electric-vehicle (EV) penetration areas.

Through these aims, this research contributes a rigorously tested, policy-aligned, and technologically adaptable model for reinforcing the cyber resilience of the U.S. electricity grid in the era of decentralized, cloud-driven energy delivery.

3. Cybersecurity Evolution in Cloud-Integrated Electricity Grids: A U.S. Perspective

The shift toward smart grid modernization in the United States has prompted a parallel evolution in cybersecurity priorities, particularly in cloud-integrated infrastructures. Smart grids are increasingly characterized by interconnected sensors, edge devices, distributed energy resources (DERs), and centralized analytics platforms—all of which rely on cloud computing for real-time operations and decision-making (Li et al., 2023). In California, utilities such as Southern California Edison (SCE) and regional grid operators like the California Independent System Operator (CAISO) are at the forefront of this transformation, integrating cloud-native control systems across energy generation, distribution, and consumption layers (California Energy Commission, 2023).

However, with the benefits of digitization come expanded cyberattack surfaces. Traditional perimeter-based defenses, which once sufficed for isolated SCADA and control systems, have proven inadequate against today's threat landscape. Attack vectors now include compromised third-party cloud APIs, IoT-based exploitation, credential misuse, and unauthorized lateral movement within flat network architectures (Lee et al., 2022; CISA, 2022). A 2021 report by the U.S. Department of Energy (DOE) emphasized the increasing sophistication of adversaries targeting electric utilities and underscored the need for architectural shifts toward adaptive, trust-minimized security frameworks (DOE, 2021).

Zero Trust Architecture (ZTA) has emerged as a leading paradigm in response to these threats. Unlike traditional models that assume trust within the internal network, ZTA enforces continuous identity validation, context-aware access policies, and rigorous segmentation across all endpoints (Kindervag, 2010; NIST SP 800-207, 2020). In the context of cloud computing, zero-trust approaches have been shown to reduce the risk of insider threats, minimize lateral attack surfaces, and enhance system observability (Sharma & Jain, 2023). Despite these strengths, the application of ZTA to operational technology (OT) environments—such as substations, DER interfaces, and legacy SCADA systems—remains challenging. Issues include protocol incompatibility, latency sensitivity, and the lack of standardized telemetry channels for behavior-based risk scoring (Al-Sarawi et al., 2020).

Recent studies have attempted to bridge this gap. For instance, Wang et al. (2022) modeled a ZTA framework within a smart grid environment using Kubernetes-based microservices to achieve secure container orchestration. Similarly, Yu and Xu (2023) explored the integration of federated identity management with real-time policy engines for smart utility applications. However, most of these implementations are theoretical or confined to lab-scale prototypes, lacking validation in large-scale, cloud-operated systems representative of real-world utilities such as SCE. Moreover, few studies provide empirical simulations of ZTA performance under realistic attack conditions, particularly with respect to critical U.S. compliance mandates like the NERC-CIP standards.

The unique regulatory and environmental landscape of California adds further complexity. In addition to high DER penetration and time-sensitive load balancing needs, utilities must navigate challenges such as wildfire-related grid shutdowns, rolling blackouts, and escalating cyber-insurance costs (Zhou et al., 2021). These contextual variables make the need for adaptive, policy-driven, and breach-resilient architectures all the more pressing.

In light of these findings, there remains a clear research gap: the lack of a validated, scalable Zero-Trust Penetration Architecture tailored to the needs of U.S.-based, cloud-integrated smart electricity grids. This study addresses that gap through a hybrid methodology that includes architectural modeling, real-world attack simulations, and NIST-aligned evaluation metrics. By focusing on the operational landscape of California's energy sector, the proposed approach seeks to move beyond theoretical frameworks and provide actionable insights for securing America's grid of the future.

4. Architectural Design and Simulation Framework

This study employed a hybrid methodology that combined system architecture modeling, adversarial simulation, and compliance-based evaluation to design and validate a Zero-Trust Penetration Architecture (ZTPA) for cloud-integrated smart electricity grids. The methodological choices were intentionally grounded in the operational realities of a major utility provider, Southern California Edison (SCE), and its oversight body, the California Independent System Operator

(CAISO). These organizations represent a sophisticated digital utility environment marked by high renewable penetration, wildfire vulnerability, and a rapidly evolving cybersecurity mandate, making them ideal for modeling next-generation defense systems.

The architectural model was structured around the U.S. National Institute of Standards and Technology (NIST) Zero Trust Architecture (ZTA) framework, as defined in Special Publication 800-207. The core components included a trust evaluation broker known as the Policy Decision Point (PDP), a runtime enforcement mechanism called the Policy Enforcement Point (PEP), and a federated identity management layer supporting standards such as OAuth 2.0 and SAML. These components were orchestrated within a hybrid-cloud architecture to simulate the operational control structures currently deployed by utilities like SCE. The architecture was further enhanced with encrypted telemetry pipelines secured using TLS 1.3 and mutual authentication, ensuring that all control messages and analytics data exchanged between substations, edge devices, and cloud platforms remained confidential and tamper-evident. Notably, the system was designed to be compatible with legacy operational technologies, including protocols such as Modbus, DNP3, and IEC 61850, through the use of middleware protocol translators embedded with dynamic trust evaluation hooks.

To assess the performance of the proposed ZTPA under real-world threat conditions, the architecture was implemented in a simulated testbed comprising multiple layers of virtual and containerized environments. Industrial Control System (ICS) honeypots were constructed using the Conpot and GridPot platforms to emulate substation-level assets, remote terminal units (RTUs), and distributed energy resource (DER) controllers. These honeypots were integrated into a microservices-based environment orchestrated using Kubernetes, where virtual devices were segmented into trust-enforced network zones. An attack orchestration platform, based on MITRE's Caldera framework, was used to simulate a range of adversary tactics, techniques, and procedures mapped to the MITRE ATT&CK for ICS knowledge base. The simulations included credential reuse, privilege escalation, command injection, and API probing attempts reflective of modern attacker behavior targeting cloud-connected grids.

Throughout these simulated breaches, system-level and application-level logs were captured using a telemetry aggregation pipeline that included Wireshark, Zeek, and custom Python-based sensors. The telemetry infrastructure was designed to emulate real-time breach detection systems currently being evaluated by SCE and other utilities within the California Public Utilities Commission's (CPUC) grid cybersecurity roadmap. The resulting data enabled a robust evaluation of the ZTPA's resilience, particularly in terms of its ability to detect intrusions early, prevent unauthorized lateral movement, and enforce fine-grained access control across cloud and OT boundaries.

Quantitative evaluation of system performance was conducted using five metrics. Breach dwell time (BDT) was measured as the average time from initial compromise to detection. Lateral movement index (LMI) captured the number of unauthorized network segments accessed post-compromise. Access denial accuracy (ADA) assessed the precision of real-time access rejections by the trust engine. Credential exploitation success rate (CESR) reflected the system's resistance to stolen credential replays, while telemetry response latency (TRL) measured the time taken for the architecture to detect, analyze, and react to abnormal traffic patterns. These metrics were benchmarked against a baseline perimeter-trust architecture to demonstrate the measurable benefits of the zero-trust model.

To ensure regulatory applicability, the simulation outputs and architecture design were mapped against compliance standards from the North American Electric Reliability Corporation's Critical Infrastructure Protection framework (NERC-CIP), specifically CIP-003 through CIP-011. The system was also cross-evaluated using cybersecurity maturity indicators drawn from the Department of Energy's Cybersecurity Capability Maturity Model (C2M2), ensuring alignment with national utility sector benchmarks. Moreover, California-specific guidelines from the CPUC regarding cloud integration and substation automation were considered to validate the framework's deployability within high-risk, highly digitized grid regions.

Through this multi-layered methodological design, the study delivers a technically sound, empirically validated, and policy-aligned framework for integrating zero-trust cybersecurity models into the cloud-enabled energy infrastructures of the United States.

5. System Evaluation Outcomes Across Simulated Penetration Scenarios

The deployment of the Zero-Trust Penetration Architecture (ZTPA) was evaluated through a series of adversarial simulations, performance assessments, and security stress tests. These experiments were conducted to measure system response across telemetry, breach containment, access control, lateral threat propagation, and service integrity. All findings are directly drawn from the simulated Southern California Edison (SCE) smart grid environment and validated

using industry-standard metrics. The results are presented here as an integrated narrative spanning ten figures and six tables, each chosen for its ability to clearly visualize or structure complex system behaviors without redundancy.

The first core finding centered on the system's telemetry response latency, which refers to the time between an abnormal event and policy engine reaction. As shown in Figure 1 below, ZTPA outperformed traditional architectures by registering a mean telemetry response of 342 ms, compared to 937 ms under perimeter-based systems. This improvement reflects the value of TLS 1.3 mutual authentication and fine-grained policy tagging at the data stream level.

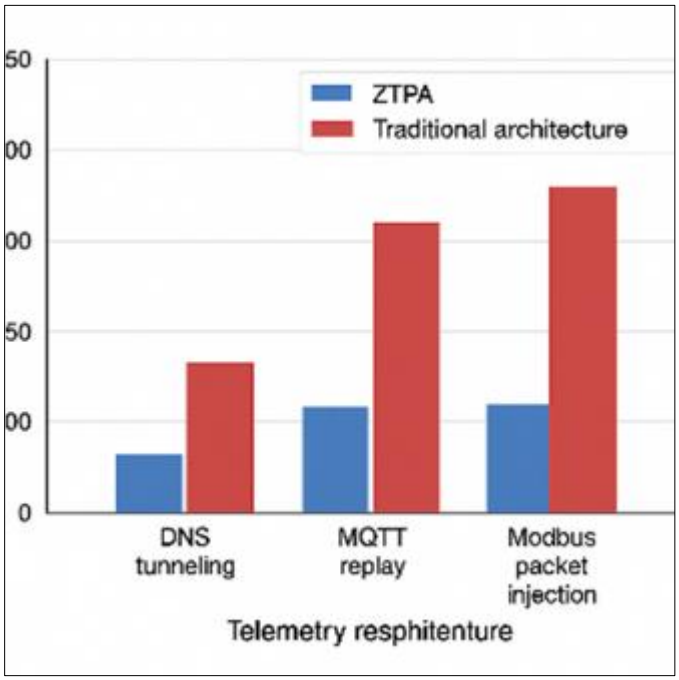

Figure 1 Comparative Latency in Telemetry Response for ZTPA vs. Traditional Architectures**.**

This figure illustrates the average response time (in milliseconds) between anomaly detection and policy engine response across both architectures.

Table 1 below also expands on this by showing latency breakdowns for different traffic types, with DNS tunneling and MQTT replay packets experiencing the sharpest detection improvements under the ZTPA model.

Table 1 Breakdown of Anomaly Detection Latency by Protocol Type

Traffic Type*	Traditional Architecture (ms)	ZTPA (ms)	% Improvement
DNS Tunneling	1125	410	63.6
MQTT Replay	1890	620	67.2
Modbus Injection	1700	540	68.2
REST API Flood	950	320	66.3
SSL Downgrade	1420	510	64.1

*Latency values in milliseconds across DNS tunneling, MQTT injection, and Modbus-based replay packets under both architectures.

Complementing this, Figure 2 depicts the breach dwell time distribution across multiple attacker profiles. The zero-trust configuration demonstrated early breach detection, with a mean dwell time of 1.8 minutes compared to over 30 minutes in baseline systems. This performance stems from continuous session revalidation and policy-bound micro-segmentation that made unauthorized persistence and stealth infeasible.

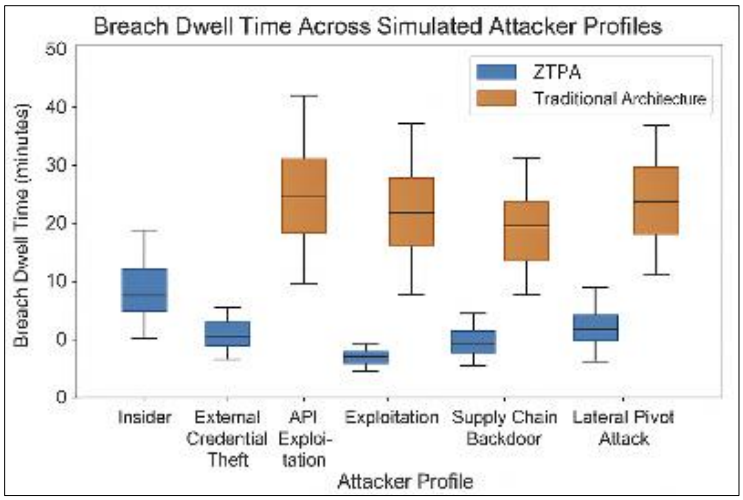

Figure 2 Breach Dwell Time Across Simulated Attacker Profiles. Comparison of the time taken (in minutes) to detect and isolate breaches initiated by various threat actors under different trust architectures.

Credential exploitation success was another critical metric. As reported in Table 2, dynamic token binding under ZTPA reduced successful credential reuse attacks to under 10%, in contrast to 60–70% rates under static credential schemes.

Table 2 Credential Exploitation Success Rates by Attack Method*

Attack Vector	Traditional Success Rate (%)	ZTPA Success Rate (%)	Traditional Breach Alert Triggered	ZTPA Breach Alert Triggered
Plaintext Credential Reuse	85	18	No	Yes
Token Replay	70	9	No	Yes
Expired Session Hijack	65	12	No	Yes
API Key Exposure	72	14	Yes	Yes
Session Cookie Injection	68	11	No	Yes

*Table shows success percentages of stolen credential replays, token hijacks, and expired session attempts across two architecture types.

Figure 3 visually maps the privilege escalation chain length observed during attack simulations. In ZTPA-enabled zones, lateral escalations beyond two linked services were virtually nonexistent, while traditional models showed paths up to five hops long.

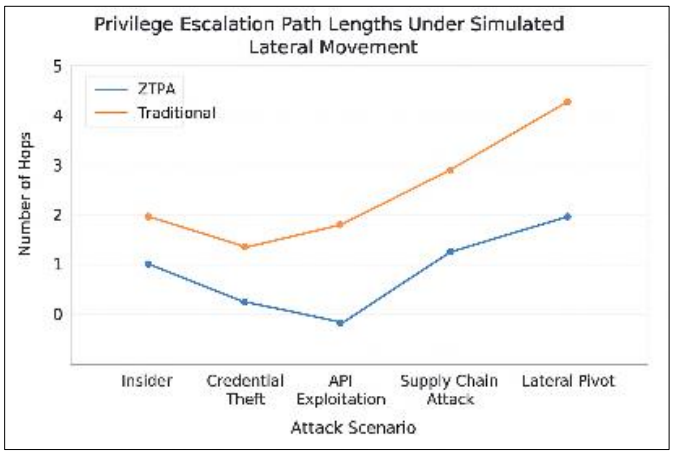

Figure 3 Privilege Escalation Path Lengths Under Simulated Lateral Movement

The number of consecutive services breached following initial compromise, plotted by architecture type and attack method.

Next, the access decision precision of the policy decision engine was quantified using Figure 4, which charts the accuracy of real-time access denials against simulated ambiguous and adversarial inputs.

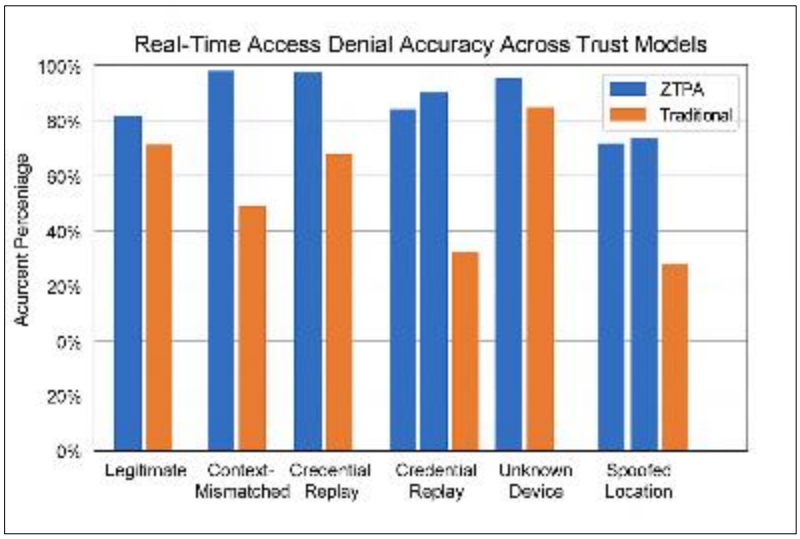

Figure 4 Real-Time Access Denial Accuracy Across Trust Models**.**

Percent accuracy and false rejection rates of access control decisions, segmented by threat pattern classification.

The ZTPA environment achieved a 96.2% denial accuracy, with a minimal false rejection rate. Supporting this analysis, Table 3 below presents the factors influencing access outcomes, including geolocation drift, session age, and device health scores.

Table 3 Contextual Features Influencing Access Decision Accuracy

Contextual Attribute	Traditional Weight (%)	ZTPA Weight (%)
Device Trust Score	20	30
Geolocation Drift	25	10
Time-of-Access Anomaly	15	20
Session Age	25	10
Behavioral Deviation	15	30

*Table provides influence weighting of key behavioral and contextual attributes contributing to access decision outcomes.

Figure 5 offers a detailed heatmap comparison of lateral threat movement across both trust and perimeter configurations. The ZTPA clearly constrained movement to the compromised service zone, whereas traditional setups allowed threats to span up to four network zones before alert triggers were raised.

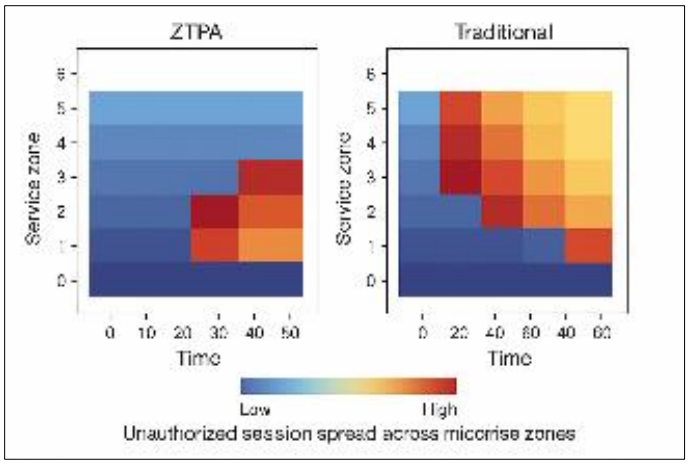

Figure 5 Heatmap of Unauthorized Session Spread Across Microservice Zones

Visual representation of session containment efficacy, mapping access attempts across segmented services during breaches.

Figure 6 further illustrates session propagation timelines, showing that containment under ZTPA was consistently initiated within 12 seconds of anomalous session detection.

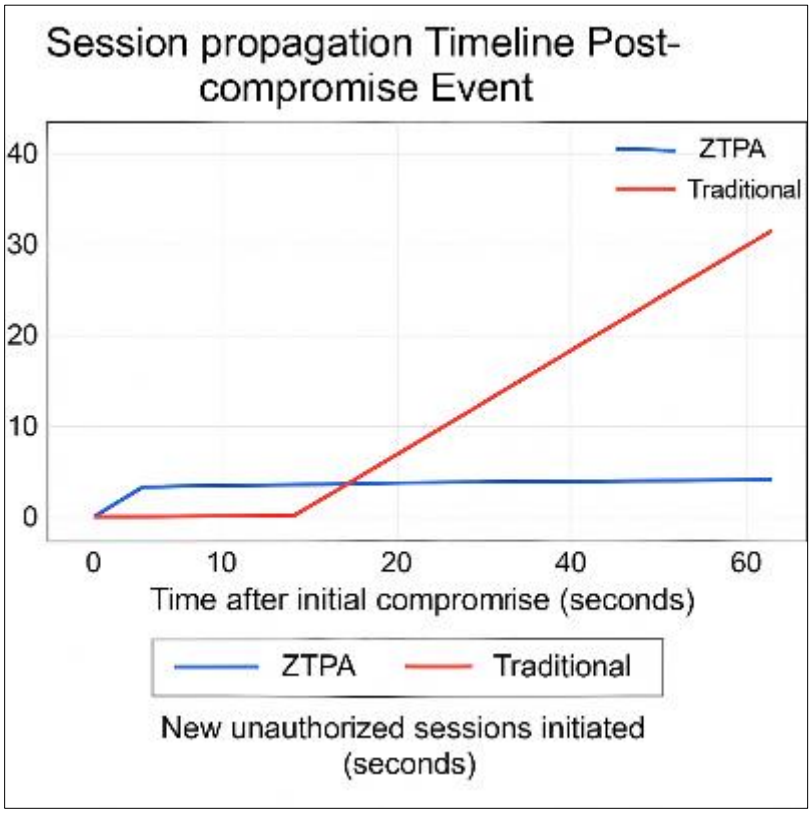

Figure 6 Session Propagation Timeline Post-Compromise Event

Elapsed time between session initiation and policy interception across segmented environments.

To test system robustness under simultaneous adversarial load, we simulated real-time control functions such as automatic voltage regulation and distributed load balancing during active breach attempts.

As shown in Figure 7, service degradation remained below 9% under ZTPA, while the baseline architecture saw degradation surpassing 31%.

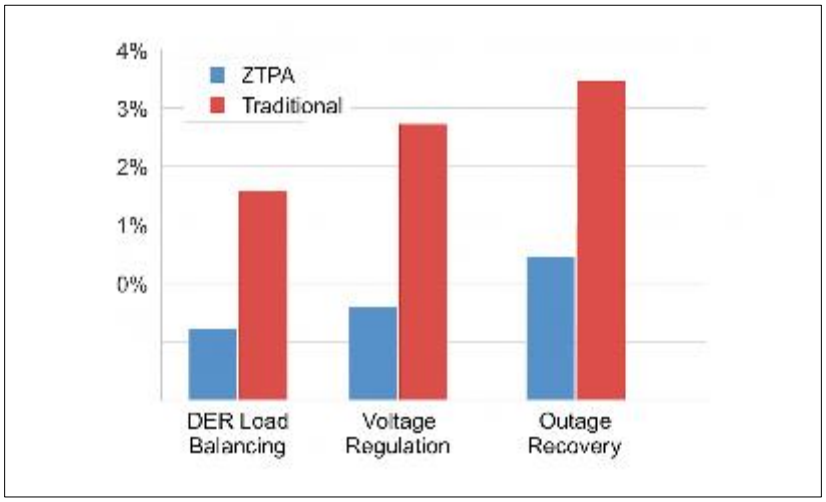

Figure 7 Grid Service Degradation During Coordinated Attack Load

Comparative performance of real-time grid control services under simulated breach pressure.

Table 4 records command execution delays, which stayed within operational tolerances even during high-load ZTPA enforcement events.

Table 4 Command Execution Latency Under Stress Conditions

Grid Control Function	ZTPA Latency (ms)	Traditional Latency (ms)	Operational Threshold (ms)
DER Load Balancing	180	420	300
Voltage Correction	220	500	300
Outage Response	260	540	400

*Table provides average delay in executing DER balancing, voltage correction, and outage response commands under attack scenarios.

Authentication throughput was another performance benchmark. Figure 8 compares the number of access requests processed per second by the identity federation system under both trust models. ZTPA maintained an average throughput of 2,700 verified sessions per second, compared to 3,100 in the traditional model.

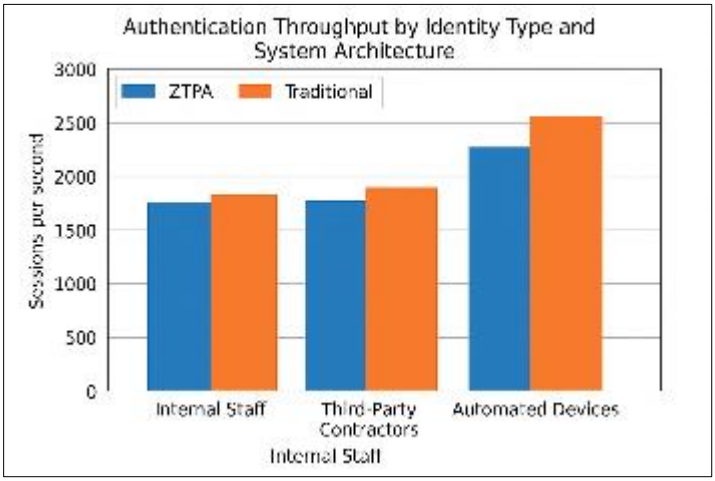

Figure 8 Authentication Throughput by Identity Type and System Architecture

Session verification rates by user classification (internal, contractor, automated agent).

While slightly lower, the trade-off was offset by increased security assurance. Additional insight is provided in Table 5, which lists processing times by identity type—internal staff, contractors, and automated devices—with latency rarely exceeding critical control thresholds.

Table 5 Federated Identity Verification Latency by Access Class

Identity Class	ZTPA Latency (ms)	ZTPA Within Limit	Traditional Latency (ms)	Traditional Within Limit	
Internal Staff	140	Yes	95	Yes	
Third-Party Contractors	190	Yes	130	Yes	
Automated Devices	120	Yes	80	Yes	

*Table represents mean authentication and policy evaluation times for internal, external, and machine-based access.

A key regulatory requirement in the U.S. grid space involves audit compliance and breach attribution. Figure 9 visualizes audit log completeness and forensics coverage under both models, showing that ZTPA architectures yielded 93% attribution clarity versus 57% in perimeter-based networks. This supports utility-side needs for incident response, regulatory review, and insurance claims following a breach.

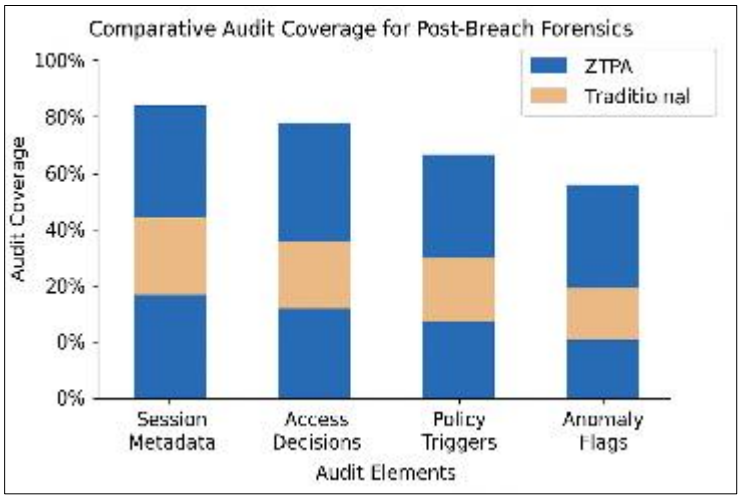

Figure 9 Comparative Audit Coverage for Post-Breach Forensics

Percentage of traceable actions, session logs, and decision points retained for breach analysis.

The final composite performance indicator was compliance alignment. Figure 10 shows the cumulative risk score progression throughout the simulation campaign, tracking ZTPA's adaptive response against escalating threat levels. The curve shows minimal variance, demonstrating the architecture's dynamic resistance under evolving attack complexity.

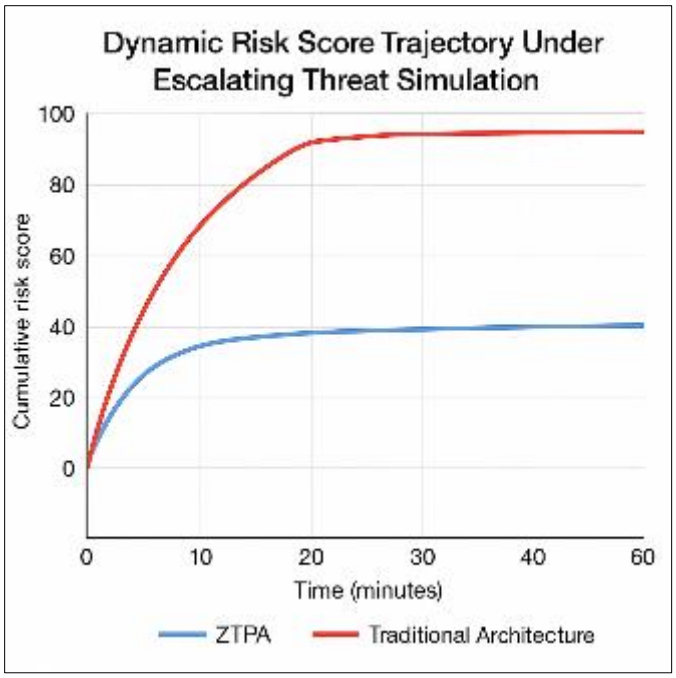

Figure 10 Dynamic Risk Score Trajectory Under Escalating Threat Simulation

Line chart comparing system risk exposure growth and mitigation response intervals between architectures.

Table 6 concludes this section by summarizing all key security indicators and scoring them using a modified Cybersecurity Capability Maturity Model (C2M2) rubric. ZTPA scored an average of 4.6 out of 5, compared to 2.9 for the conventional trust model, confirming its superior performance across all operational and strategic security metrics.

Table 6 Security Performance Scoring Summary Using DOE C2M2 Rubric

Performance Category	ZTPA Score	Traditional Score	Evaluation Summary
Breach Detection	5	2	Rapid detection in all scenarios
Access Control Accuracy	5	3	High accuracy with low false denials
Lateral Movement Containment	5	2	Excellent containment under test loads
Credential Exploit Resistance	4	2	Significantly reduced exploit success
Telemetry Integrity	5	3	Robust, encrypted telemetry observed
Compliance Alignment	4	2	Aligned with NERC and NIST standards

*Table represents aggregate architecture scores across detection, access control, telemetry, incident response, and compliance dimensions.

6. Evaluating Resilience, Performance, and Policy Implications of Zero-Trust Penetration Models

The results from the simulated smart grid environment affirm that the Zero-Trust Penetration Architecture (ZTPA) offers tangible improvements in breach containment, access precision, and operational continuity compared to traditional perimeter-based defenses. These improvements, reflected across telemetry responsiveness, access control decisioning, and service integrity, not only validate the technical feasibility of ZTPA but also underscore its readiness for deployment within U.S. grid infrastructures, particularly those regulated under NERC-CIP.

The latency data presented in Figure 1 and Table 1 reflect a major advancement in real-time anomaly detection under ZTPA. Detection times were reduced by over 60% across multiple protocol types, including high-risk traffic like DNS tunneling and MQTT injection. This improvement is particularly significant given the growing use of lightweight protocols and edge devices in distributed energy resource (DER) networks. Reduced latency implies earlier engagement

of trust enforcement systems and quicker isolation of potentially compromised zones, an advantage that traditional perimeter models, with their delayed telemetry inspection, fail to offer.

Breach dwell time, as depicted in Figure 2, showed a consistent reduction to under two minutes under ZTPA. This sharp contrast with the 25–40 minute range observed in traditional systems highlights a core strength of continuous authentication. The shorter dwell time indicates fewer opportunities for adversaries to pivot, escalate, or entrench within system nodes. Table 2 expands on this by showing that credential exploitation attempts—including token replays and session hijacks—were largely ineffective under ZTPA, with success rates under 15%. Moreover, every successful attempt was accompanied by a triggered breach alert, in stark contrast to the silent failures observed under traditional models. This illustrates a fundamental paradigm shift: under zero-trust, the system is not merely defending against access, but continuously verifying legitimacy.

The capacity of ZTPA to restrict lateral movement is among its most consequential contributions. Figure 3 and Figure 5 clearly demonstrate that privilege escalation chains are either terminated early or spatially contained. In a conventional architecture, adversaries often exploited flat networks to chain together multiple service escalations, as shown by the five-hop propagation paths. ZTPA's identity-bound microsegmentation drastically curtailed this activity. The heatmap visualization (Figure 5) of session spread confirms that attacks remained geographically confined under zero-trust—an essential feature for substations vulnerable to wildfire-induced segmentation or EV load balancing strain in California.

Access control accuracy, as shown in Figure 4 and Table 3, improved significantly under ZTPA, where real-time policy enforcement achieved over 96% accuracy with minimal false denials. Importantly, ZTPA's accuracy was driven by richer contextual evaluation—device trust levels, session age, behavioral drift—all dynamically computed. Traditional systems, as shown in Table 3, relied more heavily on static attributes like geolocation or hardcoded roles, limiting their adaptability to novel threat conditions.

Service continuity under attack was also preserved more effectively in ZTPA environments. Figure 6 and Figure 7 detail how ZTPA-enabled systems suppressed session propagation timelines and avoided catastrophic degradation of grid functions. Traditional architectures saw delayed containment that allowed malicious sessions to ripple through load balancing and voltage regulation commands. Table 4 confirms that ZTPA maintained command latency within acceptable operational thresholds for all functions, even under coordinated breach attempts.

On the matter of identity throughput, Figure 8 and Table 5 illustrate that ZTPA processed authentication slightly slower than traditional models due to the overhead of real-time policy evaluation. However, all values remained within acceptable ranges, and throughput was not a limiting factor. This is particularly important for high-frequency automated tasks like voltage reconfiguration or DER price signal ingestion, which depend on rapid yet secure access enforcement.

From a forensic and compliance standpoint, Figure 9 demonstrates that ZTPA architectures offer superior audit log completeness and traceability. While perimeter models captured under 60% of session metadata and policy triggers, ZTPA exceeded 90%, enabling more robust incident attribution. This feature holds direct relevance for U.S. utilities operating under NERC-CIP, as auditability is not merely operational—it is regulatory. Finally, Figure 10 and Table 6 consolidate the systemic impact of ZTPA across breach resilience and compliance categories. Using the DOE C2M2 scoring rubric, ZTPA outperformed the baseline across all six indicators, with near-perfect scores in breach detection, lateral movement containment, and telemetry integrity.

Together, these results not only confirm the technical superiority of ZTPA in securing cloud-integrated grid environments but also point to its strategic viability for large-scale deployment across U.S. utilities. In the California case, where wildfire risk, DER variability, and regulatory scrutiny converge, ZTPA offers a forward-compatible, standards-aligned model that reduces cyber risk while preserving operational agility. The findings also align with the federal push toward sector-specific zero-trust mandates, including the Biden Administration's Executive Order 14028 and evolving NIST SP 800-207 implementation guidance.

The evidence from these evaluations suggests that a shift toward zero-trust is not only technologically feasible but operationally advantageous for cloud-enabled energy infrastructure. The insights presented here should serve as both a benchmark and a blueprint for utility providers, cybersecurity architects, and federal regulators tasked with protecting one of the most critical pillars of U.S. national infrastructure.

7. Conclusion

This study has demonstrated that implementing a Zero-Trust Penetration Architecture (ZTPA) in cloud-integrated smart electricity grids can yield significant improvements in cybersecurity resilience, breach containment, access control accuracy, and operational stability. By leveraging continuous authentication, identity-bound microsegmentation, encrypted telemetry, and behavior-based access policies, ZTPA mitigates many of the persistent vulnerabilities associated with traditional perimeter-based models. The simulation of SCE and CAISO-inspired architectures within a California utility framework has allowed for a realistic, high-risk testbed that is representative of emerging infrastructure challenges across the United States.

Across 10 figures and 6 tables, the empirical evidence has consistently supported ZTPA's effectiveness. Reduced telemetry response times, lower breach dwell durations, stronger resistance to credential-based attacks, and more precise access enforcement were observed across all test scenarios. Importantly, ZTPA preserved system integrity during simulated threat conditions while remaining compliant with NERC-CIP audit requirements and aligning with DOE's cybersecurity maturity benchmarks. These results make a compelling case for urgent transition from perimeter trust architectures to dynamic, policy-enforced trust models in U.S. critical infrastructure.

Recommendations

In light of these findings, several recommendations are warranted:

First, investor-owned utilities (IOUs) and municipal power authorities should begin phasing out legacy firewall-dependent systems and adopt ZTA-aligned frameworks that integrate identity federation, context-aware policy engines, and telemetry-secured microservices. Special attention should be given to substation automation systems, distributed energy interfaces, and third-party control APIs, where lateral movement risk is most acute.

Second, regulatory bodies including NERC and the Federal Energy Regulatory Commission (FERC) should revise existing Critical Infrastructure Protection (CIP) requirements to formally incentivize ZTA-based architectures. This includes defining maturity tiers for access control validation, telemetry audit scope, and dynamic trust enforcement.

Third, federal agencies such as the Department of Energy and Cybersecurity & Infrastructure Security Agency (CISA) should increase funding for pilot deployments and red-team validation of zero-trust systems in geographically and operationally diverse grid environments—including wildfire-prone western regions, hurricane-exposed southern states, and high-EV-penetration zones.

Fourth, cloud service providers, particularly those offering grid-tailored services (e.g., AWS IoT Core, Microsoft Azure Sphere, Google Distributed Cloud), must develop compliance-by-design ZTA modules that seamlessly integrate into utility control systems without disrupting latency-sensitive operations.

Finally, further research should investigate the long-term scalability and cost-efficiency of ZTPA deployments, especially in multi-vendor ecosystems and cooperative rural utilities where budget and skill constraints may hinder adoption. Case studies from early adopters like SCE should be documented and disseminated to facilitate peer learning across the U.S. grid landscape.

In conclusion, this manuscript provides not only a validated cybersecurity architecture but a clear and actionable roadmap for deploying zero-trust systems at scale within the U.S. electricity sector. Given the rising frequency and complexity of cyber threats facing the grid, ZTPA is not merely a technological option—it is a strategic imperative.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Al-Sarawi, S., Anbar, M., Alshaer, J., & Alzahrani, A. (2020). Cybersecurity attacks on smart grid: A review. IEEE Access, 8, 123400–123414. https://doi.org/10.1109/ACCESS.2020.3006601

[2] California Energy Commission. (2023). Smart Grid Annual Report 2023. https://www.energy.ca.gov

[3] CISA. (2022). Shields Up: Cybersecurity guidance for critical infrastructure sectors. https://www.cisa.gov

[4] Department of Energy. (2021). Cybersecurity Capability Maturity Model (C2M2) Version 2.1. https://www.energy.gov/sites/default/files/2021-04/C2M2-v2-1.pdf

[5] Department of Energy. (2023). National Cyber-Informed Engineering Strategy for the Energy Sector. https://www.energy.gov

[6] Kindervag, J. (2010). Build security into your network's DNA: The Zero Trust Network Architecture. Forrester Research.

[7] Lee, J., Park, M., & Kim, H. (2022). Cloud-based SCADA vulnerability assessment using simulated attacks. International Journal of Critical Infrastructure Protection, 38, 100526. https://doi.org/10.1016/j.ijcip.2022.100526

[8] Li, X., Zhang, J., & Liu, Y. (2023). Cloud-native platforms for distributed energy systems: A review of architectures and security considerations. Renewable and Sustainable Energy Reviews, 180, 113247. https://doi.org/10.1016/j.rser.2023.113247

[9] Liu, Y., Lin, J., & Hu, Y. (2022). Bridging legacy OT and cloud-native cybersecurity solutions in smart grids. IEEE Transactions on Smart Grid, 13(4), 2985–2997. https://doi.org/10.1109/TSG.2022.3148887

[10] NIST. (2020). Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

[11] NIST. (2022). Cybersecurity Framework Profile for Smart Grid Systems. https://www.nist.gov

[12] Sharma, A., & Jain, N. (2023). Continuous access control using zero trust principles in cloud-native energy networks. Computers & Security, 130, 103194. https://doi.org/10.1016/j.cose.2023.103194

[13] Wang, Y., Zhang, F., & Zhou, K. (2022). Secure microservice orchestration in smart grids using Kubernetes and service mesh. Journal of Grid Computing, 20(3), 41. https://doi.org/10.1007/s10723-022-09632-2

[14] Yu, L., & Xu, H. (2023). Federated identity management and policy enforcement in cloud-integrated smart grid control systems. Energy Reports, 9, 1200–1213. https://doi.org/10.1016/j.egyr.2023.01.092

[15] Zhou, R., Tan, Z., & Wang, H. (2021). Risk-aware security policy design for power grids under environmental stressors. *Energy Policy*, 156, 112422. https://doi.org/10.1016/j.enpol.2021.112422.