**Journal of Information Systems Engineering and Management**
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Zero Trust Architecture in Mission-Critical Systems: From Perimeter Security to Continuous Verification

Yesu Vara Prasad Kollipara
Independent Researcher, USA

**ARTICLE INFO**

Received:03 Sept 2025

Revised:09 Oct 2025

Accepted:19 Oct 2025

**ABSTRACT**

Higher-risk organizations in health care, finance, and law enforcement are experiencing increasing cybersecurity risk that threatens the traditional perimeter-based security model. Zero Trust Architecture (ZTA) involves a fundamental shift in the way we think about security. ZTA eliminates trust assumptions, fixes legacy trust-based security models, and shifts to a model that assumes every access request must be verified, and does so across every request regardless of where the request originates. The "never trust, always verify" model that ZTA operates in extends to all interactions with devices, applications, and machine-to-machine communications, expanding the security coverage to the overall ecosystem. The incorporation of artificial intelligence expands ZTA as well as behavior analytics, anomaly detection, and modifying policies in a real-time sense of risk. Organizations will be able to identify unusual behavior and mitigate access for the normal user of those systems, instead of static Non-PJudicial Acquisition access. Using ZTA in higher-risk organizations has settled operations since its inception and demonstrated effectiveness in breach prevention, regulatory compliance, and overall operational resiliency. ZTA is centered upon identity, micro-segmentation, and least-privilege principles that are rooted in identity, which greatly lowers the attack surface, and is transparent to normal operating system availability. ZTA is a critical piece of infrastructure for organizations that deal with sensitive data and critical operations. ZTA provides a tangible way forward in moving towards a sustainable model for establishing systemic trust and an institution's credibility, especially as organizational ecosystems become increasingly complex and threatened.

**Keywords:** Zero Trust Architecture, Mission-Critical Systems, Continuous Authentication, Adaptive Security, AI-Driven Access Control

## 1. Introduction: Transitioning From Perimeter Defenses to Continuous Verification Models

### 1.1 Development of Boundary-Focused Security Frameworks

Cybersecurity strategies during the latter part of the 20th century and the earlier portion of the 21st century were largely defined by a focus on creating secure network perimeters. Organizations would deploy firewalls and DMZs (demilitarized zones) and institute intrusion prevention systems to create distinct boundaries around known internal trusted zones and unmatched external zones. These architectural choices indicated an operational philosophy whereby once a user or device was authenticated at a given inlet, they would be given broad trust to operate privy to internal resources. Monitoring and verifying actions would occur on infrequent occasions, often with security teams more focused on stopping unauthorized external ingress vs. authenticating and validating actions as appropriate, rather than approving the activity currently associated with given users and devices.

### 1.2 Weaknesses Inherent in Location-Based Trust Models

Contemporary adversarial strategies have taken advantage of inherent vulnerabilities associated with perimeter-centric security perspectives. Attackers using pilfered credentials, phishing activity, or compromised supply chains traverse the external defenses while masquerading as sanctioned users, once inside [1]. After initial access, they take advantage of the lower levels of scrutiny applied to an identified entity in custody of an organization to achieve extensive lateral movements and data

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

exfiltrated. As organizations realize the benefits of cloud computing, potential remote workers, and the necessity of third parties to connected services, the previously well-defined edges of networks have faced evolving threats and security in today's digital landscapes.

| Security Aspect | Perimeter-Based Model | Zero Trust Architecture |
|---|---|---|
| Trust Assumption | Implicit trust inside the network boundary | No implicit trust anywhere |
| Verification Frequency | Single authentication at the entry point | Continuous verification throughout the session |
| Access Scope | Broad access after initial authentication | Minimal permission allocation per request |
| Network Segmentation | Flat internal network structure | Micro-segmentation with isolated zones |
| Primary Control Mechanism | Network location and IP addresses | Identity credentials and behavioral context |
| Lateral Movement | Unrestricted within trusted zones | Restricted by policy enforcement points |
| Threat Detection | Perimeter monitoring focused | Continuous behavioral analytics throughout |

Table 1: Evolution of Security Models - From Perimeter to Zero Trust [1, 2]

### 1.3 Characteristics of High-Consequence Operational Environments

Specific sectors operate under conditions where security failures produce disproportionately severe ramifications. Medical facilities manage electronic health records, diagnostic equipment, and pharmaceutical systems where breaches interrupt patient care and violate health information privacy regulations. Financial institutions process trillions in daily transactions across global markets, where compromises undermine economic stability and enable large-scale fraudulent transfers. Public safety agencies maintain investigative files, intelligence communications, and civilian identification databases where unauthorized disclosures compromise active operations and constitutional privacy guarantees.

### 1.4 Core Tenets of Trust-Free Security Frameworks

Zero Trust Architecture fundamentally restructures access control by eliminating assumptions about trustworthiness based on network position [1]. Each resource request undergoes rigorous identity confirmation and permission evaluation regardless of origin point [2]. This verification requirement extends uniformly to human users, hardware endpoints, software services, and machine-to-machine communications. Authorization decisions synthesize multiple signals, including verified identity credentials, endpoint security compliance status, historical behavior patterns, and real-time threat intelligence, replacing standing access grants with narrowly scoped, session-limited permissions.

### 1.5 Scope and Organization of Present Discussion

The following sections examine the implementation of trust-free security architectures within sectors managing sensitive operations and regulated data. Content addresses foundational architectural elements, integration of machine learning technologies for adaptive threat detection, practical obstacles encountered during deployment in regulated industries, and documented security improvements across healthcare, banking, and public safety implementations. Concluding remarks synthesize observed benefits and project future development trajectories for continuous verification frameworks in high-stakes computing environments.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

## 2. Structural Elements and Core Principles of Trust-Free Security Models

### 2.1 Perpetual Validation, Minimal Permission Allocation, and Network Partitioning

Trust-free security frameworks rest upon three interconnected operational doctrines that challenge conventional access paradigms. Perpetual validation requires repeated identity confirmation and permission assessment throughout active sessions rather than relying on a single entry-point authentication [3]. Minimal permission allocation constrains user and system entitlements to precisely what specific operations demand, eliminating excess privileges that broaden vulnerability exposure. Network partitioning establishes isolated functional zones with independent gatekeeping mechanisms, confining security incidents to restricted segments and obstructing unauthorized traversal across organizational infrastructure [4].

### 2.2 Identity Confirmation, Permission Assessment, and Persistent Oversight

Robust trust-free deployments synchronize three interdependent protective operations. Identity confirmation establishes entity legitimacy through layered verification combining password credentials, hardware tokens, and biological markers [3]. Permission assessment determines whether confirmed identities hold valid entitlements for requested actions based on assigned responsibilities, situational variables, and calculated risk levels. Persistent oversight tracks ongoing system interactions, identifying irregular patterns and rule violations that trigger permission withdrawals or supplementary authentication demands [4].

### 2.3 Credential-Focused Protection Versus Location-Focused Protection

Conventional location-focused methodologies allocate trust according to network positioning, presuming entities inside defended perimeters merit unobstructed resource access. Credential-focused approaches anchor security determinations on verified entity identities independent of network placement [3]. This reorientation acknowledges contemporary computing realities where distinct boundaries no longer exist, as personnel access assets from varied locations using multiple endpoints across diverse network pathways. Validated credentials become the principal control mechanism, with permission choices tied to authenticated identities rather than IP addresses or geographic positioning [4].

### 2.4 Decision Nodes and Enforcement Nodes in Access Control

Trust-free architectures partition access governance into separate operational elements. Decision nodes assess incoming requests against established security rules, threat data, and situational factors to produce approval or rejection outcomes [3]. Enforcement nodes execute judgments rendered by decision nodes, physically regulating asset availability and blocking illegitimate attempts. This functional separation permits unified policy administration while distributing control implementation throughout infrastructure, guaranteeing uniform security standards regardless of asset location or connection methodology [4].

| Component | Primary Function | Key Capabilities | Implementation Requirements |
|---|---|---|---|
| Policy Decision Point (PDP) | Evaluate access requests against security policies | Risk assessment, contextual analysis, threat intelligence integration | Centralized policy management, real-time data processing |
| Policy Enforcement Point (PEP) | Execute access control decisions | Block/allow traffic, session termination, request forwarding | Distributed deployment, low-latency operation |

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

| | | | |
|---|---|---|---|
| Identity Provider | Authenticate entity credentials | Multi-factor authentication, credential validation, identity federation | Secure credential storage, integration with directory services |
| Continuous Monitoring System | Track ongoing activities and behaviors | Anomaly detection, pattern recognition, and audit logging | Behavioral baseline establishment, data analytics platform |
| Micro-segmentation Controller | Isolate network zones | Traffic filtering, zone isolation, and lateral movement prevention | Network virtualization, dynamic policy application |

Table 2: Zero Trust Architecture Core Components and Functions [3, 4]

### 2.5 Universal Application Across Personnel, Endpoints, Applications, and Automated Processes

Trust-free doctrines apply consistently to every participant within digital environments. Personnel undergo credential validation and obtain restricted permissions matching occupational duties and immediate circumstances [3]. Endpoint evaluation examines device security settings, software currency, and regulatory adherence before authorizing connectivity. Software applications authenticate mutually using encryption certificates and interface credentials, removing assumed trust between program modules. Automated system communications encounter equivalent validation requirements, preventing corrupted infrastructure from exploiting service credentials for illegitimate activities [4].

## 3. Intelligent Automation in Trust-Free Architectures: Machine Learning Integration

### 3.1 Incorporating Computational Intelligence into Trust-Free Security Ecosystems

Computational intelligence fundamentally alters how trust-free systems operate by enabling autonomous decision-making capabilities. Algorithmic models process extensive repositories of behavioral data, traffic metadata, and incident histories to detect sophisticated compromise indicators that traditional rule sets overlook [5]. These intelligent mechanisms continuously evolve their analytical capabilities as adversarial tactics shift, sustaining defensive efficacy against novel attack methodologies. Embedding cognitive technologies into trust-free infrastructures permits organizational scaling while diminishing reliance on human-driven security administration [6].

### 3.2 Pattern Recognition and Deviation Identification Through Algorithmic Analysis

Pattern recognition establishes normative operational profiles for personnel, hardware, and software under standard conditions. Algorithmic systems compare ongoing activities against these established profiles, highlighting irregularities suggesting stolen credentials, malicious insiders, or infiltrated infrastructure [5]. Deviation identification examines multiple situational factors, including temporal access patterns, requested resource categories, origination points, and transaction sequences. When observed behaviors substantially diverge from historical norms, automated mechanisms initiate supplementary verification procedures or impose temporary access restrictions pending administrative review [6].

### 3.3 Adaptive Permission Management and Threat-Calibrated Verification

Threat-calibrated verification adjusts authentication stringency proportional to computed danger levels accompanying particular access attempts. Routine scenarios involving recognized hardware, standard operational hours, and ordinary resource interactions proceed with streamlined verification [5]. Elevated-risk circumstances marked by atypical geographic origins, classified data requests, or questionable antecedent activities invoke rigorous authentication protocols demanding multiple validation methods. Algorithmic models perpetually recalibrate danger assessments, incorporating

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

aggregated intelligence feeds, institutional security directives, and instantaneous contextual indicators [6].

### 3.4 Algorithmic Approaches for Hostile Activity Recognition and Countermeasures

Supervised algorithmic techniques leverage annotated datasets containing documented attack signatures, facilitating swift categorization of hostile conduct when comparable activities occur. Unsupervised methodologies uncover novel threat manifestations by isolating statistical aberrations within traffic flows and conduct datasets [5]. Reinforcement-based algorithms refine defensive tactics through cyclical evaluation processes, autonomously modifying protective interventions according to measured effectiveness. These synergistic approaches enable anticipatory threat neutralization before adversaries accomplish their intended objectives [6].

| ML Technique | Application in Zero Trust | Threat Detection Capability | Operational Benefit |
|---|---|---|---|
| Supervised Learning | Classification of known attack patterns | Rapid identification of documented threats | Swift categorization of hostile conduct |
| Unsupervised Learning | Discovery of novel anomalies | Detection of previously unknown threats | Isolation of statistical aberrations |
| Reinforcement Learning | Optimization of response strategies | Adaptive defensive measure refinement | Autonomous intervention modification |
| Behavioral Analytics | Establishment of normative profiles | Credential theft and insider threat detection | Deviation identification from baselines |
| Risk Scoring Algorithms | Dynamic authentication adjustment | Context-aware threat level computation | Threat-calibrated verification stringency |

Table 3: Machine Learning Techniques in AI-Enhanced Zero Trust [5, 6]

### 3.5 Instantaneous Security Rule Modification Driven by Situational Awareness

Adaptive governance engines harness algorithmic intelligence to alter permission frameworks dynamically, absent manual administrative action. When threat recognition models detect heightened danger conditions, rule modification systems automatically strengthen security configurations by curtailing entitlements, intensifying verification cadence, or quarantining implicated network zones [5]. Conversely, when danger metrics decrease and conduct patterns stabilize, systems progressively reinstate conventional access privileges to limit operational interference. This situational flexibility sustains protective effectiveness while maintaining workforce efficiency across fluctuating threat environments [6].

## 4. Deployment Obstacles and Strategic Planning for High-Consequence Computing Environments

### 4.1 Antiquated Infrastructure Compatibility and Historical System Constraints

Introducing trust-free frameworks into existing technological environments encounters significant hurdles related to aging infrastructure capabilities. Antiquated software platforms and hardware components typically lack built-in mechanisms for contemporary credential validation, fine-grained permission structures, and persistent activity surveillance [7]. These installations originated during periods emphasizing boundary-focused protection philosophies rather than credential-based verification models. Adapting historical infrastructure toward trust-free operational standards necessitates careful assessment of authentication intermediary solutions, communication protocol

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

converters, and graduated transition approaches preserving service availability while incrementally advancing security postures [8].

### 4.2 System Responsiveness and Processing Delays in Continuous-Operation Platforms

High-consequence operations require unbroken service delivery and minimal transaction delays, generating friction with trust-free frameworks introducing supplementary validation stages. Iterative credential checks, instantaneous policy assessments, and conducting analysis computations impose computational burdens that potentially degrade system responsiveness [7]. Medical facilities conducting diagnostic procedures, financial organizations performing rapid transaction execution, and public safety agencies orchestrating emergency coordination cannot accept authentication postponements hampering time-critical functions. Architectural approaches must reconcile security thoroughness with responsiveness demands through streamlined policy mechanisms, distributed computing placements, and data retention tactics minimizing delay consequences [8].

### 4.3 Institutional Adaptation Requirements and Personnel Interaction Consequences

Migrating toward trust-free paradigms necessitates profound cultural adjustments extending beyond technical infrastructure alterations. Staff familiar with frictionless internal connectivity frequently interpret amplified authentication occurrences and permission constraints as efficiency obstacles [7]. Security intervention points disrupting established workflows cultivate personnel opposition, potentially motivating circumvention practices undermining protective intentions. Effective transitions demand thorough educational initiatives, forthright explanations regarding security justifications, optimized authentication interactions, and progressive enhancement informed by personnel observations to sustain institutional buy-in while accomplishing security targets [8].

### 4.4 Statutory Requirement Coordination Across Regulated Industries

Trust-free deployments within governed sectors must fulfill rigorous compliance structures dictating information safeguarding and permission oversight. Medical organizations conforming to HIPAA directives encounter explicit mandates for activity documentation, permission mechanisms, and incident disclosure protocols [7]. Banking entities satisfying PCI-DSS specifications must exhibit protected payment information handling and infrastructure isolation. Public safety organizations observing CJIS Security Policy confront prescribed authentication benchmarks and facility protection obligations. Trust-free frameworks must correspond accurately with statutory requirements while furnishing verifiable compliance evidence through exhaustive documentation and reporting capabilities [8].

### 4.5 Financial Justification and Investment Prioritization for Trust-Free Adoption

Institutions contemplating trust-free integration must weigh considerable upfront commitments against anticipated sustained security enhancements. Deployment outlays encompass platform procurement, equipment modernization, consulting engagement for architectural planning, personnel education, and continuous operational expenditures for surveillance and upkeep [7]. High-consequence settings encounter supplementary costs addressing redundancy mandates, validation procedures, and risk containment protocols throughout conversion intervals. Economic validation demands measuring prospective incident cost prevention, statutory sanction avoidance, operational effectiveness improvements, and reputation preservation advantages against implementation expenses and perpetual operational charges [8].

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

| Challenge Category | Specific Obstacles | Impact on Operations | Mitigation Strategies |
|---|---|---|---|
| Legacy System Integration | Lack of modern authentication protocols, outdated architectures | Service disruption risk, compatibility gaps | Authentication bridge technologies, phased migration approach |
| Performance Requirements | Added verification latency, computational overhead | Transaction delay, system responsiveness degradation | Streamlined policy mechanisms, edge computing, and caching strategies |
| Organizational Adaptation | User resistance, workflow disruption | Productivity impediments, circumvention behaviors | Comprehensive training, transparent communication, iterative refinement |
| Regulatory Compliance | HIPAA, PCI-DSS, and CJIS alignment requirements | Audit complexity, documentation burden | Exhaustive logging, automated compliance reporting, and policy mapping |
| Resource Allocation | Initial investment costs, ongoing operational expenses | Budget constraints, ROI uncertainty | Cost-benefit quantification, breach cost avoidance measurement |

Table 4: Implementation Challenges and Mitigation Strategies in Mission-Critical Environments [7, 8]

## 5. Documented Implementations and Performance Indicators Across High-Consequence Industries

### 5.1 Medical Sector: Protected Health Information Safeguarding and Statutory Compliance Enhancement

Healthcare organizations adopting trust-free security frameworks exhibit strengthened defenses protecting confidential patient records and improved adherence to privacy regulations. Perpetual validation protocols restrict illegitimate entry to electronic medical documentation, imaging repositories, and pharmaceutical ordering platforms [8]. Trust-free structures implement precise permission boundaries guaranteeing clinical staff obtain exclusively information pertinent to immediate care obligations. Layered credential verification, combined with conducting surveillance, diminishes vulnerabilities from stolen authentication tokens and malicious internal actors targeting protected medical data. Comprehensive activity documentation inherent within trust-free deployments furnishes extensive evidence supporting statutory compliance verification throughout regulatory inspections [8].

### 5.2 Banking Operations: Deceptive Transaction Mitigation and Statutory Requirement Satisfaction

Financial establishments incorporating trust-free protection models accomplish quantifiable reductions in illicit transaction execution and unlawful account manipulation. Ongoing authentication mechanisms identify credential theft endeavors and account hijacking operations before adversaries finalize illegitimate fund movements [8]. Conduct examination algorithms that recognize transaction sequences diverging from typical customer profiles, invoking supplementary validation procedures to prevent unauthorized monetary withdrawals. Trust-free designs support compliance with payment card industry specifications through infrastructure isolation, separating transaction processing zones and exhaustive access documentation, recording all cardholder information interactions. These functionalities concurrently reinforce deception prevention while fulfilling demanding regulatory supervision obligations [8].

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

### 5.3 Public Safety Operations: Restricted Information Defense and Evidence Documentation Integrity

Government enforcement organizations embracing trust-free doctrines strengthen safeguards surrounding investigative documentation, intelligence transmissions, and legal evidence repositories. Detailed permission structures confine restricted information visibility exclusively to certified personnel, demonstrating confirmed operational necessity [8]. Thorough activity tracking generates permanent examination records documenting every engagement with confidential case materials, reinforcing custody documentation requirements critical for judicial proceedings. Trust-free infrastructures obstruct unauthorized horizontal progression throughout enforcement communication networks, isolating potential incidents within partitioned zones and defending active investigations from infiltration. Stratified authentication procedures fulfill criminal justice information security mandates while preserving operational effectiveness throughout urgent public safety interventions [8].

### 5.4 Numerical Performance Indicators: Incident Frequency Decline and Detection Interval Compression

Institutions deploying trust-free infrastructures document considerable advancements in quantifiable protection performance benchmarks. Security breach occurrence diminishes as perpetual validation and infrastructure partitioning constrain adversary progression following initial penetration [8]. Recognition capabilities augmented through conduct examination and irregularity identification compress the duration separating intrusion commencement and security personnel notification. Mechanized reaction protocols activated by policy infractions expedite containment interventions, curtailing residence duration throughout which opponents extract confidential materials or broaden infrastructure penetration. These numerical enhancements convert immediately into decreased incident correction expenditures and reduced statutory penalty vulnerability [8].

### 5.5 Non-Quantifiable Advantages: Stakeholder Confidence, Regulatory Assurance, and Continuity Strength

Extending beyond calculable protection benchmarks, trust-free installations produce wider institutional benefits, influencing organizational standing and constituent connections. Augmented information safeguarding capabilities fortify public assurance toward institutions administering confidential personal details [8]. Regulatory authorities cultivate heightened certainty concerning organizational protection frameworks when observing thorough trust-free mechanisms and exhaustive compliance evidence. Operational continuity advances as partitioned designs prevent isolated vulnerability points from propagating throughout complete infrastructures. These non-quantifiable advantages accumulate throughout prolonged intervals, establishing competitive distinctions for institutions exhibiting superior protection methodologies within corresponding sectors [8].

## Conclusion

Zero Trust Architecture (ZTA) represents a decisive shift in cybersecurity philosophy—moving from static, perimeter-based defenses to continuous, verification-driven security models that align with today's complex threat landscape. As mission-critical industries such as healthcare, finance, and law enforcement face increasingly sophisticated adversaries, traditional trust boundaries have proven insufficient against attacks exploiting implicit access assumptions. Trust models that are free from implied deception are expanded by using artificial intelligence to enable reactive behavioral analytics, automated feedback adjustment, and detection of emerging threats and changing baselines of operation. While these frameworks have obstacles to live deployments, which include legacy systems that are not always optimized for a smooth integration, large and relevant performance logged considerations, changing organizational cultures, and aligning regulatory adherences, which add difficulty. There have been documented deployments that show evidence of not only improved breach prevention capabilities, improved speed in detecting incidents, but also adherence to regulations.

Regardless of measurable safety deviations and metrics of security practices, free-trust frameworks enhance reputational factors in your organization, regulatory trust, and confidence in operational resilience through the provision of services in a high-consequence environment. A key factor in moving away from trust practices based on location and auditing approaches, with later identification based on practices anchored to identity-based verification, with strengthening measures put in place to prevent further leverage of sensitive materials and/or services. In an environment where digital footprints reach fuller inter-connections and the capacity of adversaries becomes more competitive, free trust practices will be a standard designed element of infrastructure for organizations actively managing high-consequence operations and cultivating public trust in the increasing threats of known and unknown environments.

## References

[1] Kai Li, Conggai Li, et al., "Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things," IEEE Transactions on Network and Service Management (preprint), March 2025. Available: https://www.tkn.tu-berlin.de/bib/li2025zero-trust/li2025zero-trust.pdf
[2] Ebuka Mmaduekwe Paul et al., "Zero Trust Architecture and AI: A Synergistic Approach to Next-Generation Cybersecurity Frameworks," International Journal of Science and Research Archive, vol. 13, no. 2, December 24, 2024. Available: https://ijsra.net/sites/default/files/IJSRA-2024-2583.pdf
[3] Naeem Firdous Syed et al., "Zero Trust Architecture (ZTA): A Comprehensive Survey," IEEE Access, vol. 10, May 12, 2022. Available: https://ieeexplore.ieee.org/document/9773102
[4] Muhammad Liman Gambo, Ahmad Almulhem, "Zero Trust Architecture: A Systematic Literature Review," arXiv preprint arXiv:2503.11659, March 21, 2025. Available: https://arxiv.org/html/2503.11659v2
[5] Hrishikesh Joshi, "Emerging Technologies Driving Zero Trust Maturity Across Industries," IEEE Open Journal of the Computer Society, November 22, 2024. Available: https://ieeexplore.ieee.org/stampPDF/getPDF.jsp?arnumber=10764723
[6] Saubhagya Munasinghe et al., "Machine Learning Based Zero Trust Architecture for Secure Networking," in 2023 IEEE 17th International Conference on Industrial and Information Systems (ICIIS), September 20, 2023. Available: https://ieeexplore.ieee.org/document/10253610/keywords#keywords
[7] Peter M. Curtis, Maintaining Mission Critical Systems in a 24/7 Environment, Third Edition, Wiley-IEEE Press, 2020. Available: https://ieeexplore.ieee.org/book/9295052
[8] Baozhan Chen et al., "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," IEEE Internet of Things Journal, vol. 8, no. 13, July 1, 2021. Available: https://ieeexplore.ieee.org/document/9273056