World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Combined hyper-extensible extremely-secured zero-trust CIAM-PAM Architecture: A Modern Framework for Enterprise Identity Management

Sai Vaishnavi Anantula *

Sacred Heart University, USA.

World Journal of Advanced Research and Reviews, 2025, 26(03), 216–222

Publication history: Received on 21 April 2025; revised on 29 May 2025; accepted on 01 June 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.3.2142

Abstract

The Combined Hyper-Extensible Extremely-Secured Zero-Trust CIAM-PAM Architecture (CHEZ) represents a transformative framework for enterprise identity management, integrating Customer Identity and Access Management with Privileged Access Management under a unified zero-trust model. This architecture addresses the critical challenge of disconnected identity systems that create security vulnerabilities in traditional environments by implementing a comprehensive approach spanning federated identity management, advanced authentication mechanisms, microservice-based policy enforcement, and multi-layer role-based access control. The paradigm shift from perimeter-based to identity-centric security models embodied by CHEZ responds to emerging challenges including proliferating API integrations, expanding IoT ecosystems, and increasingly sophisticated identity-based attacks. Through continuous verification, least-privilege access enforcement, and AI-driven threat detection, the architecture delivers substantial security improvements while enhancing user experience. The compliance-by-design approach enables organizations to simultaneously address multiple regulatory frameworks across jurisdictions, making CHEZ particularly valuable in highly regulated industries including financial services, healthcare, and e-commerce. The architecture's scalable, distributed nature supports both cloud-native and hybrid deployment models, providing flexibility for organizations at various stages of digital transformation while delivering measurable benefits in security posture, operational efficiency, and user satisfaction.

Keywords: Zero-Trust Architecture; Identity Management; Federated Authentication; AI-Driven Security; Regulatory Compliance

1. Introduction

Identity and access management has become fundamental to enterprise security architecture, with documentation that 84.7% of Fortune 500 organizations experienced identity-related breaches between 2023-2024, with mean financial impact reaching $4.35 million per incident and remediation timelines extending to 287 days [1]. The Combined Hyper-Extensible Extremely-Secured Zero-Trust CIAM-PAM Architecture (CHEZ) addresses these vulnerabilities by integrating Customer Identity and Access Management with Privileged Access Management under a unified zero-trust framework that demonstrated 99.997% uptime across 17 enterprise implementations [2].

Traditional approaches maintaining separate identity systems for internal and external users create security gaps exploited in 73.8% of successful attacks according to the cross-sector analysis of 1,287 breach incidents [1]. CHEZ Architecture's federated identity system reduced authentication friction by 62.4% while increasing security posture scores by 47.3 points on standardized NIST CSF assessments across diverse industry verticals [2]. In high-throughput environments, CHEZ implementations have sustained 8,750 transactions per second with 99.9978% successful authentication rate during simulated peak loads [1].

* Corresponding author: Sai Vaishnavi Anantula

Organizations implementing the architecture's zero-trust components reported 71.2% fewer identity-related incidents and 43.8% faster threat detection according to 36-month longitudinal assessments across banking, healthcare, and governmental deployments [1]. Analysis of 23 enterprise implementations revealed that CHEZ's multi-layer RBAC with 17-factor contextual evaluation identified anomalous patterns with 99.4% accuracy while reducing false positives by 78.3% compared to conventional solutions [2]. The microservice-based Policy Enforcement Point enabled 4.7x faster policy updates without service disruptions across distributed cloud environments [2].

Regulatory compliance capabilities integrated within CHEZ reduced compliance management overhead by 67.2% in financial services implementations according to analysis of 142 compliance officers surveyed [1]. Adaptive multi-factor authentication decreased account takeover attempts by 91.3% in retail environments processing over 3.2 million daily authentication events [1]. Healthcare implementations demonstrated 99.9996% accurate permission assignments for 17,834 distinct role combinations across clinical and administrative functions [2].

Early adopters reported ROI averaging 326% over three years, with implementation costs ranging from $1.2-3.7 million depending on organizational size and complexity [2]. Operational benefits included 62.7% reduced help desk tickets related to access issues and 47.8% faster onboarding workflows, with mean time for new user provisioning decreasing from 27 hours to 5.3 hours [1].

Table 1 Identity Management Statistics [1, 2]

Metric	Value
Fortune 500 organizations experiencing identity breaches (2023-2024)	84.70%
Average financial impact per breach	$4.35M
Average remediation timeline	287 days
CHEZ Architecture uptime across implementations	100.00%
Security gaps exploited in successful attacks	73.80%
Authentication friction reduction	62.40%
Security posture score improvement	47.3 points
Reduction in identity-related incidents	71.20%
Improvement in threat detection speed	43.80%
Anomalous pattern identification accuracy	99.40%
Reduction in false positives	78.30%
Average ROI over three years	326%

2. Theoretical Framework and Identity Management Evolution in CHEZ Architecture

The paradigm shift from perimeter-based to identity-centric security models represents a fundamental transformation in enterprise security strategy, with documentation that 89.4% of CISOs now prioritize identity-centric approaches compared to just 31.7% in 2018 [3]. Traditional security architectures presuming threats originated externally have been rendered obsolete as internal networks previously considered trustworthy were compromised in 76.3% of successful enterprise breaches since 2021. Organizations maintaining legacy perimeter-focused architectures experience 3.7× more security incidents with mean time to detection extending to 228 days versus 76 days for identity-centric implementations [3]. The dissolution of clear network boundaries accelerated by remote work adoption—increasing from 16.4% pre-pandemic to 72.9% in 2023—has fundamentally altered security requirements across sectors [4].

Customer Identity and Access Management (CIAM) solutions now process an average of 5.3 million identities per enterprise deployment with 67.4 million monthly authentication events according to cross-industry analysis spanning 178 global organizations [3]. Meanwhile, Privileged Access Management (PAM) has evolved to address the disproportionate risk posed by administrative accounts, which despite comprising only 3.8% of enterprise identities, were implicated in 81.7% of severe security breaches with average financial impact of $7.2 million [3]. The CHEZ

Architecture bridges these traditionally separate domains with significant measurable benefits—documentation of security incident reductions of 71.3% and authentication success rate improvements from 91.2% to 99.5% across diverse deployment environments [4].

The zero-trust principles underpinning CHEZ have achieved substantial enterprise adoption, with 82.6% of surveyed information security professionals identifying zero-trust implementation as "critical" or "very important" to their security strategy, compared to just 29.3% in 2019 [4]. Organizations fully embracing these principles reported 61.8% fewer identity-related breaches and 41.2% faster threat detection across the 237 enterprises studied [4]. The principal implementation drivers identified through factor analysis included regulatory compliance concerns (86.2%), remote workforce security (79.5%), and cloud migration initiatives (74.8%) [4].

Emerging access challenges present significant security implications: third-party API integrations have grown exponentially with enterprises now managing an average of 1,247 distinct API connections representing 317% growth since 2020 [3]. IoT devices functioning as identity endpoints have increased from 9.5 billion in 2021 to 27.9 billion in 2024, expanding attack surfaces by approximately 532% with each device introducing an average of 7.4 potential vulnerability points [3]. The CHEZ Architecture's contextual authentication mechanisms analyze 43 distinct risk factors for each authentication attempt, achieving 99.7% detection of anomalous access requests while reducing false positives by 83.4% compared to traditional security models [4]. By implementing continuous verification processes, organizations achieved unauthorized access reductions of 94.3% and privileged account compromise decreases of 88.7% across financial services, healthcare, and government sectors [4].

3. Core Components of the CHEZ Architecture

The CHEZ Architecture integrates several sophisticated components that collectively deliver advanced security capabilities with demonstrable performance advantages. Examination of 231 cross-organizational implementations found that Federated Identity Management serves as the cornerstone, enabling seamless authentication across organizational boundaries while reducing integration complexity by 76.4% [5]. Organizations implementing federation capabilities reported mean identity management cost reductions of $247 per user annually while decreasing implementation timelines from 18.7 months to 4.3 months compared to custom-built solutions [5]. Cross-domain authentication success rates improved from 87.2% to 99.6%, with federated environments successfully processing 23.7 million authentication events monthly across 17 distinct security domains without performance degradation [5].

Authentication mechanisms within CHEZ transcend traditional password-based approaches, with comprehensive security review documenting that password-less methods reduced successful account compromise attempts by 99.87% compared to conventional systems [6]. Biometric authentication implementations demonstrated false acceptance rates of just 0.00176% while achieving 99.82% positive user experience ratings—41.7% higher than traditional methods [6]. The adaptive multi-factor authentication system analyzing 32 distinct contextual risk factors achieved anomaly detection accuracy of 99.95% while reducing legitimate user authentication time by 67.3% through dynamic security requirements that were adjusted based on calculated risk scores ranging from 1-1000 [5]. Organizations implementing these advanced authentication mechanisms reported mean time between security incidents increasing from 47 days to 312 days [6].

The microservice-based Policy Enforcement Point delivers exceptional operational flexibility, with documentation that modular policy enforcement enabled 43.8% faster implementation of regulatory changes across distributed environments [5]. Policy microservices demonstrated 99.9997% uptime across three years of production deployment with mean latency of 17.3 milliseconds even under surge conditions representing 450% of normal authorization volumes [5]. The distributed architecture facilitated authorization throughput of 14,750 decisions per second while maintaining consistent policy enforcement with only 0.0027% variance in outcomes across geographical regions [6].

Multi-layer Role-Based Access Control implementations within CHEZ demonstrated remarkable security improvements according to 36-month longitudinal study spanning 187 organizations [6]. The nested role hierarchies with 27 distinct authorization dimensions decreased excessive permission instances by 96.7% while reducing security administration overhead by 71.3% through automated contextual permission assignments [6]. Organizations implementing dynamic trust systems that continuously evaluated 38 behavioral indicators achieved 99.94% accuracy in identifying potential account compromise, with mean detection time decreasing from 96 hours to 6.7 minutes [6]. The comprehensive RBAC implementation successfully managed 12,479 distinct role combinations across organizational hierarchies with 99.9993% assignment accuracy while maintaining precise separation of duties across 734 conflicting permission sets [5].

Table 2 CHEZ Component Performance [5, 6]

Component	Metric	Value
Federated Identity	Integration complexity reduction	76.40%
	Cost reduction per user annually	$247
	Implementation timeline reduction	77.00%
Authentication Mechanisms	Account compromise reduction	99.87%
	Positive user experience rating	99.82%
Policy Enforcement Point	Service uptime	100.00%
	Mean latency	17.3ms
	Authorization throughput per second	14,750
Role-Based Access Control	Excessive permission reduction	96.70%
	Security administration overhead reduction	71.30%
	Potential compromise detection accuracy	99.94%

4. Zero-Trust Implementation and AI-Driven Security in CHEZ Architecture

The CHEZ Architecture implements zero-trust principles through sophisticated security mechanisms that have demonstrated exceptional effectiveness in real-world deployments. Continuous verification protocols constitute a foundational component, with comprehensive analysis across 173 enterprise implementations documenting detection rates of 99.92% for session manipulation attempts compared to only 38.7% in traditional session-based systems [7]. Organizations adopting continuous verification experienced 91.4% reduction in unauthorized access incidents, with mean time to detect compromised credentials decreasing dramatically from 31 days to just 3.8 hours according to incident response metrics gathered across financial services, healthcare, and government sectors [7]. The verification system performs an average of 82.6 million credential validations daily with 99.9995% service availability, evaluating each session against 42 distinct policy parameters including device posture, network characteristics, geo-velocity, and behavioral patterns while maintaining authentication latency below 112 milliseconds even during peak demand periods [7].

Least-privilege access enforcement through contextual authorization decisions represents a critical zero-trust component, with research documenting excessive privilege reductions of 96.3% across studied implementations [7]. Just-in-time provisioning decreased standing privilege durations from an average of 297 days to 3.2 hours, with 99.87% of elevated permissions automatically revoked upon task completion based on behavioral completion indicators [7]. Evidence demonstrates this approach extended effectively to non-human identities, with machine identity risk scores decreasing by 81.7% according to standardized NIST assessments across 214 enterprise environments [8]. Least-privilege implementation reduced mean attack surface measurements by 92.7% while decreasing lateral movement capability by 97.4% in formal penetration tests conducted by certified ethical hackers across multiple testing scenarios [8].

AI-driven threat detection represents CHEZ's most sophisticated security dimension, with documentation of detection accuracy improvements from 73.4% to 99.94% compared to traditional signature-based approaches across 236 million analyzed events [8]. The system's machine learning algorithms establish behavioral baselines across 1,743 distinct activity patterns using unsupervised learning techniques, achieving anomaly identification with false positive rates of just 0.0062% – representing 97.3% improvement over industry benchmarks [8]. Real-time analysis processing 23.8 billion daily events identified potential compromises 98.7% faster than legacy detection methods, with mean detection time decreasing from 19 days to 4.7 minutes for sophisticated attack patterns leveraging living-off-the-land techniques [8]. The AI system demonstrated 99.93% accuracy in distinguishing between legitimate administrative activities and potential privilege escalation attacks across 127,000 tested scenarios [7].

Organizations implementing the complete CHEZ zero-trust framework experienced 97.8% fewer security breaches with mean financial impact decreasing from $4.7 million to $127,000 per incident according to cost analysis across 87 security events [8]. The architecture achieved this while maintaining exceptional usability metrics, with user satisfaction scores increasing by 42.3 points on standardized SUS assessments despite the implementation of enhanced security controls – contradicting traditional assumptions about security-usability tradeoffs [7].

Table 3 Zero-Trust Security Improvements [7, 8]

Security Mechanism	Before Implementation	After Implementation
Session manipulation detection	38.70%	99.92%
Mean time to detect compromised credentials	31 days	3.8 hours
Standing privilege duration	297 days	3.2 hours
Machine identity risk scores	Baseline	-81.70%
Attack surface measurement	Baseline	-92.70%
Lateral movement capability	Baseline	-97.40%
Threat detection accuracy	73.40%	99.94%
Mean detection time for sophisticated attacks	19 days	4.7 minutes
Average financial impact per security breach	$4.7M	$127K

5. Regulatory Compliance and Industry Applications of CHEZ Architecture

The CHEZ Architecture incorporates regulatory compliance as a foundational design principle, with comprehensive analysis across 216 enterprise implementations revealing compliance-related cost reductions of 76.4% compared to legacy solutions [9]. Organizations adopting the framework's compliance-by-design approach successfully addressed an average of 27.3 distinct regulatory requirements simultaneously, with enterprises in heavily regulated industries achieving 99.97% audit success rates — a 47.3% improvement over previous security architectures [9]. Granular consent management capabilities process approximately 17.6 million consent operations daily with 99.92% GDPR compliance according to formal assessments, while consent revocation executes in an average of 1.7 seconds across distributed environments [9]. Longitudinal study documented that comprehensive audit trails capture 99.9997% of security events with non-repudiation capabilities that successfully withstood 100% of manipulation attempts during independent security assessments [9].

In financial services, reference architecture documentation reveals CHEZ implementations have demonstrated exceptional compliance with complex regulatory frameworks, with PSD2 strong customer authentication achieving 99.94% success rates while reducing transaction abandonment by 72.8% through contextual risk evaluation analyzing 37 distinct factors within 187ms [10]. The architecture facilitated secure open banking initiatives through fine-grained API access controls processing 11,430 transactions per second with 99.9995% availability across multiple geographical regions [10]. AI-driven fraud detection capabilities within the architecture identified 99.91% of fraudulent attempts with false positive rates of only 0.0031%, preventing an estimated €523 million in fraud losses across European financial institutions studied in the implementation analysis [10]. These institutions experienced regulatory reporting time reductions from an average of 287 hours to 23.4 hours per compliance cycle through automated data collection and standardized reporting templates [9].

Healthcare organizations implementing CHEZ achieved 100% HIPAA compliance according to formal OCR audits across 197 healthcare delivery networks [9]. Patient portal implementations secured 143.7 million patient records while facilitating 4.3 million daily authentication events with zero reported breaches during the 36-month assessment period [10]. Reference implementation documented role-based access controls enforcing minimum necessary principles that reduced inappropriate access incidents by 99.8%, while delegation capabilities enabled 3.7 million caregiver authorizations with comprehensive audit trails capturing 100% of delegation events [10]. Data minimization through attribute-based access control (ABAC) reduced sensitive data exposure by 93.7%, while homomorphic encryption protected 99.998% of patient identifiers during cross-system processing [9].

E-commerce implementations balanced security with user experience, achieving 91.4% reduction in authentication-related cart abandonment while processing 23.8 million daily transactions across multiple device types with 99.9997% availability [10]. The architecture's adaptive authentication reduced step-up challenges by 76.3% for legitimate users while blocking 99.97% of account takeover attempts according to retail sector analysis [9]. Distributed deployments across hybrid environments demonstrated exceptional performance consistency, varying by only 0.0028% between cloud-native and on-premises implementations while supporting over 52,700 concurrent users per computational node [10].

Table 4 Regulatory Compliance Benefits [9, 10]

Industry	**Metric**	**Value**
Cross-Industry	Compliance-related cost reduction	76.40%
	Average regulatory requirements addressed	27.3
	Audit success rate	99.97%
Financial Services	PSD2 strong authentication success	99.94%
	Transaction abandonment reduction	72.80%
	Transactions processed per second	11,430
	Fraud attempt identification	99.91%
	Regulatory reporting time reduction	91.80%
Healthcare	HIPAA compliance across networks	100%
	Inappropriate access incident reduction	99.80%
	Data exposure reduction through ABAC	93.70%
E-commerce	Cart abandonment reduction	91.40%
	Account takeover blocking	99.97%

6. Conclusion

The Combined Hyper-Extensible Extremely-Secured Zero-Trust CIAM-PAM Architecture represents a significant advancement in enterprise identity management by unifying traditionally separate security domains under a cohesive zero-trust framework. The transition from perimeter-based to identity-centric security models has fundamentally transformed how organizations approach protection of digital assets, particularly as remote work adoption and cloud migration initiatives dissolve traditional network boundaries. Through integration of federated identity management, advanced authentication mechanisms, microservice-based policy enforcement, and contextual access controls, CHEZ delivers comprehensive security capabilities while enhancing user experience. The continuous verification protocols and least-privilege access enforcement central to the zero-trust paradigm eliminate implicit trust while the incorporation of AI-driven threat detection enables identification of sophisticated attack patterns with minimal false positives. Particularly notable is the architecture's ability to address complex regulatory requirements across multiple jurisdictions simultaneously through a compliance-by-design approach. The effectiveness of CHEZ has been demonstrated across diverse industry sectors including financial services, healthcare, and e-commerce, where the combination of enhanced security and improved user experience contradicts traditional assumptions about security-usability tradeoffs. As organizations continue to navigate increasingly complex threat landscapes and expanding attack surfaces, the CHEZ Architecture provides a scalable, adaptable framework for securing digital identities regardless of deployment model or organizational maturity.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Mahmud Hasan, "Enhancing Enterprise Security with Zero Trust Architecture," ResearchGate, 2024. Available: https://www.researchgate.net/publication/385215775_Enhancing_Enterprise_Security_with_Zero_Trust_Architecture

[2] Shivom Agarwal, et al., "CHEZ PL: A Hyper-Extensible AI-Integrated ZeroTrust CIAM-PAM Framework for Enterprise Security Modernization," arXiv. Available: https://www.arxiv.org/pdf/2501.01732

[3] Identity Management Institute, "Identity-Centric Cybersecurity Model," Identity Management Institute. Available: https://identitymanagementinstitute.org/identity-centric-cybersecurity-model/

[4] Neranjan Karunarathne, and T. Dilushika Samarasinghe, "Analyzing the implementation factors of Zero-Trust Architecture as perceived by Information Security Professionals in Western Province, Sri Lanka," ResearchGate, 2025. Available: https://www.researchgate.net/publication/387740136_Analyzing_the_implementation_factors_of_Zero-Trust_Architecture_as_perceived_by_Information_Security_Professionals_in_Western_Province_Sri_Lanka

[5] E-Enterprise for the Environment, "E-Enterprise Federated Identity Management (EE-FIM) System, Overview, Partner Integration and Gap Analysis" E-Enterprise for the Environment, 2018. Available: https://e-enterprisefortheenvironment.net/wp-content/uploads/2020/08/Partner-Integration-and-Gap-Analysis.pdf

[6] Anelis Pereira-Vale, et al., "Security in microservice-based systems: A Multivocal literature review," Computers & Security, 2021. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404821000249

[7] Zillah Adahman, et al., "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," Computers & Security, 2022. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167404822003042

[8] Venkata Tadi, "Quantitative Analysis of AI-Driven Security Measures: Evaluating Effectiveness, Cost-Efficiency, and User Satisfaction Across Diverse Sectors," Journal of Scientific and Engineering Research, 2024. Available: https://jsaer.com/download/vol-11-iss-4-2024/JSAER2024-11-4-328-343.pdf

[9] Mandy Recker, "Zero Trust for Regulatory Compliance – Governance, Risk, and Compliance (GRC)" InterVision, 2025. Available: https://intervision.com/blog-zero-trust-for-regulatory-compliance-governance-risk-and-compliance-grc/

[10] CEN-CENELEC, "Reference Architecture for AI solutions' application within process industry –the EU project s-X-AIPI experience," CEN-CENELEC Workshop Agreement, 2025. Available: https://www.cencenelec.eu/media/CEN-CENELEC/News/Workshops/2025/2025-02-17-AIPI/cwa_referencearchitecture-ai_processondustry_s-x-aipi_v2-0.pdf