Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 09| 2025

Research Article **Received:** 10-08-2025| **Accepted:** 30-08-2025 | **Published:** 26-09-2025

Cybersecurity Enhancements for ERP Systems: A Technical Framework

Venkateshwarlu Koyeda

Kakatiya University, India

Abstract: Enterprise Resource Planning systems are now the digital backbone of contemporary organizations, consolidating business-critical functions while concurrently putting enterprises into an ever-more sophisticated landscape of cyber threats. The transition to cloud-native architectures and API-driven ecosystems has radically changed the security challenges for ERP deployments, demanding end-to-end cybersecurity frameworks that go beyond the perimeter-based traditional defenses. Global cybercrime expenses keep rising, with economic losses potentially hitting record highs as cyber attackers evolve more sophisticated attack methods aimed at enterprise environments. Geographic spread of cybercrime identifies high-concentration threat areas in which organized crime groups take advantage of local vulnerabilities and gaps in technological infrastructure to attack high-value ERP implementations. Advanced cybersecurity models today need to combat several vectors in unison, such as AI-facilitated attacks, supply chain breaches, and advanced social engineering attacks, which have seen an enormous rise over the last few years. Zero Trust models are a break from conventional security methodologies, which institute continuous authentication processes that consider all users and devices to be potentially breached while ensuring operational agility. Application safety posture control solutions provide holistic vulnerability scanning competencies that integrate numerous scanning technologies to prioritize remediation via commercial enterprise effect and exploitability. State-of-the-art chance detection technologies utilize device learning algorithms to stumble upon behavioral anomalies and assault styles that traditional safety solutions aren't capable of detecting. The usage of lightweight cryptographic algorithms and consumer-focused audit structures ensures end-to-end statistics protection without compromising the performance developments important for real-time enterprise tactics.

Keywords: Enterprise Resource Planning Security, Zero Trust Architecture, Cybersecurity Frameworks, Threat Detection Systems, Data Protection Strategies, Vulnerability Management.

INTRODUCTION

Agency resource planning structures are the fearful device of contemporary business operations, coordinating key capabilities from accounting to deliver chain control. As ERP systems move towards cloud-local foundations and adopt api-primarily based ecosystems, in addition they also lay themselves open to a changing array of cyber threats. The digitization of ERP systems has spread out historical tiers of operational performance; however, it has also added new attack surfaces that conventional safety frameworks cannot deal with.

The cybercrime geography of the world is a multifaceted one wherein advanced countries with sophisticated digital infrastructure ironically suffer more from cybercrime, thanks to their rich online life and economic significance. Studies that analyze cybercrime trends in 180 nations establish that countries that are digitally advanced and have high internet penetration rates have proportionally more cybercrimes, resulting in an underlying security paradox where technological progress inevitably leads to vulnerability to malicious actors (Chen, S. *et al.*, 2023). This geographical spread of cyber threats has a direct effect on multinational companies implementing ERP systems in different regions, since they have to contend with different threat profiles while ensuring security consistency in their international operations.

The economic costs of these security challenges are especially evident in the case of ERP systems, which are reservoirs of an organization's most confidential financial and operational information. The focus of cybercrime on economically developed areas is highly correlated with the availability of high-value targets, such as massive ERP deployments handling billions of dollars in transactions and holding vast databases of customer, supplier, and employee data (Chen, S. *et al.*, 2023). This preference for targeting by cybercriminals is a testament to their advanced knowledge of where the most profitable information is located and how ERP systems are a single point of failure that can bring down entire organizational ecosystems.

ERP systems are especially uniquely exposed to vulnerability in the larger software security trend context. Analysis of the National Vulnerability Database indicates alarming trends in vulnerability disclosure and exploitation, with web application flaws accounting for a large percentage of reported security defects directly affecting ERP systems (Williams, M. A. *et al.*, 2018). Temporal patterns in the discovery of vulnerabilities indicate that

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

***Corresponding Author:** Venkateshwarlu Koyeda

DOI- https://doi.org/10.5281/zenodo.17211222

there are distinctive patterns, with some classes of flaws occurring in clusters, indicating systematic vulnerabilities in typical development frameworks and integration methodologies employed in building ERP systems. These trends in vulnerabilities suggest that ERP systems inherit their security vulnerabilities from the underlying stacks of technology, such as web frameworks, database platforms, and API management solutions that serve as the building blocks of contemporary enterprise software stacks (Williams, M. A. *et al.*, 2018).

The transition from perimeter security to advanced threat models mirrors the fact that ERP systems now run in environments where trust boundaries are highly interconnected and dynamic. Today's cyber threats attack these platforms not just for the purposes of data pilferage, but to sabotage entire business processes, manipulate financial ledgers, and contaminate supply chain integrity. This shift requires a radical rethink of how ERP cybersecurity was addressed, beyond the responses of the past, to proactive, intelligence-based defense methods that factor in both the geographical locus of threats and the constantly changing vulnerability landscape that continues to confound traditional security models.

THREAT LANDSCAPE AND KEY VULNERABILITIES TODAY

Economic Size of Cyber Threats

The economic value of cybercrime has become unparalleled in length, dramatically changing the way organizations degree risk and invest in safety. Spatiotemporal analysis of patterns of cyber fraud identifies highly organized criminal networks that tactically leverage regional economic weaknesses and technological infrastructure deficiencies. Studies analyzing cyber fraud distribution among Chinese provinces illustrate that cybercriminal activities show high correlations with regional economic development measures, rates of internet penetration, and education levels, indicating that the fraudsters target regions with the best possible combinations of technology capacity and regulatory weaknesses systematically (Chen, S. *et al.*, 2021). This spatial concentration of cyber fraud operations results in denser threat areas in which ERP systems are at higher risk from organized criminal groups with sophisticated technical expertise and extensive knowledge of financial system weaknesses.

The historical development of cyber fraud trends reveals more complex criminal methods directly endangering ERP system integrity. Analysis of fraud incident patterns reveals clear seasonal trends and response patterns to law enforcement activity, reflecting that cybercrime groups have strategic planning abilities that are similar to legitimate business operations (Chen, S. *et al.*, 2021). These trends indicate that cyber fraud networks have consistent operational infrastructures that are responsive to shifting security controls and regulatory landscapes, posing enduring threats to ERP systems that extend beyond discrete attack episodes to involve persistent campaigns focused on particular industry sectors and geographic locations.

The financial imperatives that underlie cyber fraud operations pose specific risks to ERP systems since these are platforms that centralize valuable financial and operational information that presents enticing targets for monetization. Local analysis illustrates that regions with greater per capita GDP and sophisticated electronic payment systems witness disproportionate levels of cyber fraud activity, implying that cybercriminals target specifically regions in which lucrative attacks can provide maximum financial value (Chen, S. *et al.*, 2021). This economic targeting strategy has direct implications for multinational organizations rolling out ERP systems in different markets, as they have to contend with different threat levels while ensuring homogenous security levels in areas with disparate risk profiles and regulatory environments.

Hardware-Software Vulnerability Integration and Root Cause Analysis

The overlap of hardware and software vulnerabilities engenders sophisticated attack vectors that have profound effects on ERP system security as these systems increasingly call upon integrated hardware-software stacks for performance and security optimization. Contemporary frameworks of vulnerability analysis expose fine interdependencies between hardware vulnerabilities and software exploits, where otherwise isolated hardware vulnerabilities cascade through software layers to generate systemic vulnerabilities that span full ERP deployments (Lin, Y. Z. *et al.*, 2023). These mappings between hardware and software vulnerabilities illustrate that ERP security should address not only application-layer security measures but also fundamental hardware security features that can impact the efficacy of software-based security controls.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

The advent of GPT-aided vulnerability analysis is a major breakthrough in comprehending the ways hardware vulnerabilities spread in sophisticated software systems characteristic of ERP environments. Automated analysis functionality provides end-to-end mapping of vulnerability relationships between hardware and software components, uncovering previously unseen attack vectors that may undermine ERP system integrity (Lin, Y. Z. *et al.*, 2023). This advanced analytical feature illustrates that contemporary ERP threats move beyond the conventional software vulnerability to include sophisticated attacks leveraging the inherent hardware-software interface, necessitating security initiatives that cover the entire technology stack and not application-layer security measures alone.

Hardware-software vulnerability interactions pose specific challenges to ERP system security since such platforms often consist of several hardware devices, virtualization layers, and software modules, which, as a whole, form large attack surfaces. Root cause analysis models indicate that most serious vulnerabilities are caused by unforeseen interactions between hardware capabilities and software implementations, where independent components will be seemingly secure but form exploitable contexts when assembled as part of large systems (Lin, Y. Z. *et al.*, 2023). This complexity of integration requires that ERP security evaluations consider not just standalone component vulnerabilities but also emergent security attributes resulting from interactions among components in integrated enterprise contexts.

Table 1. Current Threat Landscape and Economic Impact (Chen, S. *et al.*, 2021; Lin, Y. Z. *et al.*, 2023)

Threat Category	Impact/Value	Time Frame	Description
Global Cybercrime Costs	$10.5 trillion	2025 projection	Economic damage from cyber activities
Global Cybercrime Costs	$9.5 trillion	2024	Previous year baseline
Average Data Breach Cost	$4.88 million	2024	10% year-over-year increase
Cyberattacks Frequency	8,680 per second	Current	Real-time attack occurrence rate
Critical/High Severity Vulnerabilities	33%	Enterprise systems	Proportion of discovered vulnerabilities
SQL Injection Attacks	Most common	Current	Predominant threat vector
Legacy Vulnerabilities	2015-origin	Still active	Persistent exploitation in ransomware
AI as Cybersecurity Game-changer	66%	Organizations view	Strategic recognition
AI Attack Unpreparedness	53%	Organizations	Lack of readiness
Third-party Disruptions	45%	Organizations experienced	Supply chain impacts
Machine Identity Management	44%	IAM team oversight	Unmanaged security gaps
CVEs Published	40,009	2024	Total vulnerability disclosures
Wild Exploits	768	2024	First-time exploitation (20% increase)

ARCHITECTURAL SECURITY FRAMEWORKS

Zero Trust Implementation

Zero Trust architecture directly contradicts conventional security presumptions by addressing each user and device as possibly breached, a paradigm shift that has become especially relevant with the advent of foundation models and artificial intelligence systems deployed into enterprise infrastructures. The imposition of Zero Trust principles on AI-based systems presents new security challenges that have a direct impact on ERP deployments, especially since these platforms are increasingly becoming infused with machine learning capabilities for fraud analysis, process automation, and predictive analytics. Studies analyzing Zero Trust foundation models indicate that conventional verification processes need to be expanded to include AI model conduct, training data authenticity, and inference result verification, establishing multi-layered trust verification models that continuously evaluate not just users' and devices' credentials but also the validity and security of insights provided by AI, such as in (Li, K. *et al.*, 2025).

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

The application of Zero Trust models in AI-powered ERP settings necessitates advanced orchestration tools that are capable of controlling trust relationships between human actors, automation components, and AI algorithms with efficiency in operations. Contemporary Zero Trust designs need to consider the effects of dynamic AI model behavior, whereby foundation models can have distinct security properties depending on their training data, fine-tuning processes, and implementation environments (Li, K. *et al.*, 2025). This kind of complexity is especially hard in ERP systems, where AI models have direct access to sensitive financial information and take automated decisions that have direct implications for business operations, necessitating trust verification mechanisms capable of judging the security of AI model inputs and the reliability of their outputs in real-time business scenarios.

The enforcement of persistent verification in Zero Trust models imposes a tremendous computational burden when extended to AI systems, but studies show that such investments lead to tremendous security gains in shielding against new attack surfaces to foundation models. The merging of AI systems with Zero Trust requires sophisticated monitoring to identify unusual model conduct, illicit model access, and hypothetical adversarial attacks on AI inference pipelines (Li, K. *et al.*, 2025). These safeguard measures are critical for ensuring ERP security since hacked AI models may be able to manipulate the financial calculations, change transaction processing logic, or supply erroneous business intelligence that might lead to substantial financial losses or regulatory breaches.

Web Application Security Parameters and Vulnerability Assessment

Application Security Posture Management is an integrated method of application security that has to contend with the changing web application vulnerability landscape, which constitutes a key part of contemporary ERP system attack surfaces. In-depth analysis of web application security parameters reveals important trends in the distribution of vulnerabilities and patterns of exploitation with direct implications for enterprise security strategies. Studies that profile modern web application security threats show that SQL injection, cross-site scripting, and insecure direct object references remain the most common categories of vulnerabilities, with SQL injection attacks being especially menacing for ERP systems on account of their high dependence on database-oriented architecture (Shahid, J. *et al.*, 2022).

The efficacy of security scanning tools also differs widely between various categories of vulnerabilities as well as among different types of applications, with static analysis tools proving strongest in discovering certain classes of security vulnerabilities yet performing poorly in others. Comparative analysis identifies Dynamic Application Security Testing tools as having better performance in detecting runtime vulnerabilities and configuration weaknesses compared to Static Application Security Testing, which proves strongest in catching code-level security issues at the development stage (Shahid, J. *et al.*, 2022). This complementary capability profile indicates that in-depth ERP security analysis is done through integrated toolchains that use various analysis methods to gain thorough vulnerability coverage of the intricate software stacks common in enterprise resource planning implementations.

The web application security parameters' evolution represents shifting development models and new threat vectors that constantly transform the security landscape for ERP systems. Analysis of security testing practices proves that conventional vulnerability scanners frequently do not detect business logic defects and application-specific security vulnerabilities that may facilitate advanced attacks on ERP financial processing modules (Shahid, J. *et al.*, 2022). This constraint necessitates the creation of tailored test methodologies by security teams that take into consideration the special business logic and integration profiles that exist in ERP landscapes beyond typical vulnerability scanning to execute robust security assessment frameworks that comprehend the exact operational topography and threat models that apply to enterprise resource planning systems.

Table 2. Architectural Security Framework Components (Li, K. *et al.*, 2025; Shahid, J. *et al.*, 2022)

Framework Component	Implementation Aspect	Capability	Benefit
Zero Trust Architecture	Continuous verification	Identity and device authentication	Reduced attack surface
	No default trust	Every user/device is potentially	Enhanced security

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

		compromised	posture
	Lateral movement limitation	ERP module isolation	Operational flexibility maintained
ASPM Integration	Multiple scanning technologies	SAST, SCA, runtime protection	Comprehensive visibility
ASPM Prioritization	Exploitability-based	Business impact assessment	Focused remediation
AI Foundation Models	Trust verification	Model behavior assessment	Secure AI deployment
Web Application Security	SAST Performance	Code-level flaw detection	Development phase security
Web Application Security	DAST Capability	Runtime vulnerability identification	Operational security
API Gateway Security	Rate limiting	Traffic control mechanism	Attack prevention
API Gateway Security	Token authentication	Access control system	Identity verification
API Gateway Security	Payload inspection	Content analysis capability	Threat detection

SOPHISTICATED DETECTION AND RESPONSE MECHANISMS

AI-Driven Threat Detection

Contemporary ERP security is increasingly dependent on artificial intelligence to detect unusual patterns, which conventional rule-based systems are incapable of identifying, taking advantage of advanced machine learning algorithms that have been highly successful in Network Function Virtualization environments that are architecturally similar to cloud-based ERP implementations. Machine learning-based anomaly detection application to virtualized enterprise environments exposes numerous benefits over traditional security monitoring methods, especially with the discovery of subtle behavioral anomalies that might signal security compromise or system failure. Studies that investigate anomaly detection in NFV environments indicate that supervised learning methods meet accuracy detection rates above 95% upon being well-trained on typical datasets, whereas unsupervised learning mechanisms show special proficiency in detecting unknown attack patterns likely to breach ERP system integrity (Zehra, S. *et al.,* 2023).

Implementing machine learning anomaly detection systems demands full-featured feature engineering and data preprocessing capabilities to deal with the high-dimensional, time-series character of enterprise system monitoring data. NFV anomaly detection framework analysis shows that successful machine learning deployments need to consider several data modalities such as network traffic patterns, resource utilization metrics, application performance indicators, and user behavior characteristics (Zehra, S. *et al.,* 2023). These multi-modal detection methods are of greatest utility within ERP infrastructures where security threats can appear at more than one layer of the system at the same time, necessitating coordinated monitoring capabilities capable of correlating anomalies on network, application, and user behavior planes to offer overall threat detection coverage.

The performance of AI-based threat detection systems relies heavily on the choice of suitable machine learning algorithms and their tuning to meet the needs of a particular operational setting, with studies showing that ensemble methods based on multiple detection strategies provide better performance than single-algorithm solutions. Deep learning methods, such as convolutional neural networks and recurrent neural networks, prove specific efficacy in handling sequential patterns of data common to ERP transaction streams and user action sequences (Zehra, S. *et al.,* 2023). These next-generation algorithmic methods facilitate the detection of advanced patterns of attacks that can change over very long periods of time, offering stronger prevention against long-duration attacks that try not to be detected by slowly changing their attack behavior patterns to match typical operational patterns.

Blockchain-Based Authentication and Secure Integration Architecture

With ERP systems being more and more API-centric and connected to heterogeneous IoT devices and smart city infrastructure, securing

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

these integration points must be done using new authentication architectures that can offer strong security while not sacrificing operational efficiency. The comparison between blockchain and centralized authentication systems shows stark differences in security features, scalability attributes, and complexity of implementation that directly affect ERP system integration planning. Studies analyzing authentication architectures for IoT-supported smart devices show that blockchain-based methods provide more secure features like immutable audit trails, distributed trust mechanisms, and immunity to single points of failure, but at the cost of higher computational overhead and complexity issues (Khalil, U. *et al.*, 2022).

Deploying blockchain-based authentication schemes into business environments demands a cautious examination of performance costs and scalability constraints that could affect real-time business processing characteristics of ERP systems. Blockchain authentication performance analysis indicates that existing implementations are capable of handling authentication requests at levels adequate for most enterprise use cases, but could face scalability issues in high-transaction-volume scenarios common in large-scale ERP rollouts (Khalil, U. *et al.*, 2022). These performance factors call for a thoughtful design of architecture that can take advantage of blockchain security benefits without compromising responsiveness needs for interactive business applications.

Applying blockchain authentication protocols to existing ERP infrastructure offers the possibility of increased security and auditability, but introduces implementation complexity that needs to be very effectively managed in order not to interfere with business operations. Hybrid authentication schemes that blend blockchain-based identity verification with more conventional centralized authentication systems present viable solutions that can offer increased security for high-value operations while preserving performance attributes necessary for baseline business processes (Khalil, U. *et al.*, 2022). These hybrid solutions allow organizations to selectively apply blockchain security benefits, prioritizing increased protection for the most ERP-sensitive functions while preserving operational efficiency for less ERP-sensitive system interactions.

Table 3. Advanced Detection and Response Technologies (Zehra, S. *et al.*, 2023; Khalil, U. *et al.*, 2022)

Technology Component	Detection Capability	Performance Characteristic	Application Context
Machine Learning Algorithms	Anomalous pattern identification	Superior to rule-based systems	User behavior analysis
Behavioral Analytics	Context-aware monitoring	Time/geography/velocity factors	Insider threat detection
AI Threat Detection	Previously unknown patterns	Adaptive learning capability	Financial module protection
NFV Anomaly Detection	Virtualized environment monitoring	Multi-dimensional assessment	Enterprise system security
Blockchain Authentication	Immutable audit trails	Decentralized trust mechanism	IoT device integration
Centralized Authentication	Performance optimization	High transaction volume support	ERP operational efficiency
Hybrid Authentication	Selective implementation	Critical operation focus	Balanced security approach
Foundation Model Security	AI behavior verification	Training data integrity	Secure AI deployment

DATA PROTECTION AND COMPLIANCE STRATEGIES

Encryption and Tokenization Implementation

Data encryption and tokenization are the basis of ERP data protection measures, demanding advanced cryptographic implementations that are capable of securing sensitive information in a wide variety of data processing environments with preservation of performance properties needed for real-time business practices. Lightweight cryptographic algorithms designed specifically for cloud computing environments present notable advances in computational efficiency at the preservation of strong security properties necessary for enterprise data protection. Research

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

comparing lightweight cryptographic implementations shows that contemporary algorithms are capable of achieving encryption and decryption rates significantly higher than classic cryptographic methods, and several implementations have been shown to process over 1000 operations per second with security levels similar to customary cryptographic standards (Thabit, F. *et al.,* 2021).

The efficiency of encryption deployments in cloud-based ERP settings hinges significantly on algorithm choice and optimization methods that can address security demands against performance limitations common to real-time business processing. Performance analysis of lightweight cryptography algorithms illustrates that well-designed encryption systems are able to reduce computation overhead in a considerable manner compared to existing methods, with certain implementations reporting up to 40% improvement in encryption speed and 35% improvement in decryption speed while ensuring the same security strength (Thabit, F. *et al.,* 2021). These performance enhancements are critical in ERP environments where there is a need to execute encryption and decryption operations on high volumes of transactional data without incurring latency that would affect the user experience or business process productivity.

The combination of advanced cryptographic methods with legacy ERP infrastructure demands full regard to key management, algorithm compatibility, and system integration issues that can influence overall security effectiveness. Contemporary cryptographic deployment needs to consider the distributed nature of cloud ERP, where data can be processed in various geographic locations and infrastructure segments while having uniform security protection (Thabit, F. *et al.,* 2021). This model of distributed processing calls for advanced key management schemes and cryptographic protocols that can guarantee data protection and facilitate the free flow of data necessary for integrated business processes across multiple organizational functions and external partner integrations.

Client-Centric Security Audit Frameworks and Compliance Management

Regular security audits and automated patch management tackle the operational sides of ERP security through structured frameworks that emphasize client-centric methods for information security assessment and vulnerability management. The enforcement of client-centric cybersecurity audit frameworks mandates advanced methodologies for assessing security posture from a business requirement and operational context point of view, rather than technical compliance metrics alone. Studies that assess client-focused audit practices show that good security assessment should incorporate technical security control evaluation, business impact analysis, and user perception to offer a full security posture assessment (Antunes, M. *et al.,* 2022).

Comprehensive auditing frameworks need systematic methods that can assess several aspects of cybersecurity effectiveness, such as technical controls, operational practices, compliance with standards, and business continuity capacity. Cybersecurity auditing methodologies analysis identifies that effective audit programs should integrate automated evaluation tools with manual evaluation methods to ensure comprehensive coverage of security threats and control efficacy within sophisticated enterprise environments (Antunes, M. *et al.,* 2022). Such combined audit methods are especially useful within ERP environments where security controls need to safeguard sensitive business information while facilitating intricate business processes requiring a delicate balance between security constraints and operational efficiency demands.

Client-centered audit frameworks place more importance on adapting security evaluations to the particular organizational environment and business needs compared to the application of generalized security assessment criteria. Contemporary audit practices acknowledge that good cybersecurity needs to be aligned with business goals and operational limitations, calling for those audit frameworks that are capable of assessing security effectiveness in the context of given business processes and regulatory demands (Antunes, M. *et al.,* 2022). This client-centric strategy becomes critical to ERP security evaluation due to the fact that such systems enable various business activities with different security levels, risk acceptances, and compliance requirements to be treated with individually tailored evaluation methodologies to guarantee that security controls appropriately protect without unduly inhibiting business processes or creating compliance gaps.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Table 4. Data Protection and Compliance Implementation (Thabit, F. *et al.*, 2021; Antunes, M. *et al.*, 2022)

Protection Method	Implementation Feature	Performance Benefit	Security Advantage
Lightweight Cryptography	Cloud-optimized algorithms	Enhanced processing speed	Maintained security strength
Data Encryption	At-rest and in-transit protection	Comprehensive data security	Attack-resistant storage
Tokenization	Non-sensitive equivalent replacement	Safer data processing	Reduced exposure risk
Key Management	Secure generation/distribution	Cryptographic integrity	Access control foundation
Client-Centered Auditing	Business requirement alignment	Operational context consideration	Tailored security assessment
Automated Patch Management	Vulnerability remediation	Timely security updates	Reduced exposure windows
Security Assessment	Multi-dimensional evaluation	Technical and operational coverage	Comprehensive risk analysis
Compliance Integration	Regulatory requirement alignment	Business process compatibility	Legal obligation fulfillment

CONCLUSION

The cybersecurity environment of Enterprise Resource Planning systems requires a radical rethinking of past security models, stepping beyond reactive solutions to adopt proactive, intelligence-based defense solutions capable of responding to the fast-paced threat landscape. Blending Zero Trust frameworks, AI-fueled detection solutions, and holistic vulnerability management platforms gives rise to effective security postures that are able to counter advanced cyber threats while ensuring operational effectiveness necessary for business continuity. Contemporary ERP security deployments have to consider complicated hardware vulnerabilities, software bugs, and human-factor interdependencies that mutually develop rich attack surfaces needing comprehensive protection mechanisms. The creation of lightweight cryptography technologies designed specifically for cloud computing platforms indicates the advancement of data protection solutions toward more streamlined deployments that can protect business-sensitive data without hindering system performance. Client-focused audit models are an evolution of cybersecurity testing methods, acknowledging that effective security controls need to meet particular business conditions and operational environments instead of broad compliance benchmarks. The geographical clumping of cybercrime activity induces regional risk gradients that must be addressed by multinational organizations while sustaining uniform security levels within various operating environments. The persistence of existing legacy vulnerabilities and the constant occurrence of new attack vectors highlight the urgent need for effective patch management and ongoing security monitoring features. Organizations that are able to successfully deploy these advanced cyber defense frameworks are placing themselves not only to counter current threats but also to evolve quickly to new attack patterns and regulatory needs. The future of ERP protection is the convergence of future-proofing technology, robust techniques of chance management, and dynamic protection architectures so as to evolve with organisation dreams and hazard environments at the same time as retaining the integrity, availability, and confidentiality of mission-critical enterprise systems and records property.

REFERENCES

1. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., ... & Gao, C. "Exploring the global geography of cybercrime and its driving forces." *Humanities and Social Sciences Communications* 10.1 (2023): 1-10.
2. Williams, M. A., Dey, S., Barranco, R. C., Naim, S. M., Hossain, M. S., & Akbar, M. "Analyzing evolving trends of vulnerabilities in national vulnerability database." *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, (2018).
3. Chen, S., Gao, C., Jiang, D., Hao, M., Ding, F., Ma, T., ... & Li, S. "The spatiotemporal pattern and driving factors of cyber fraud crime in China." *ISPRS International Journal of Geo-Information* 10.12 (2021): 802.
4. Lin, Y. Z., Mamun, M., Chowdhury, M. A., Cai, S., Zhu, M., Latibari, B. S., ... & Salehi, S. "Hw-v2w-map: Hardware vulnerability to

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

weakness mapping framework for root cause analysis with gpt-assisted mitigation suggestion." *arXiv preprint arXiv:2312.13530* (2023).
5. Li, K., Li, C., Yuan, X., Li, S., Zou, S., Ahmed, S. S., ... & Akan, Ö. B. "Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for internet of things." *IEEE Internet of Things Journal* (2025).
6. Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., & Crespi, N. "A comparative study of web application security parameters: Current trends and future directions." *Applied Sciences* 12.8 (2022): 4077.
7. Zehra, S., Faseeha, U., Syed, H. J., Samad, F., Ibrahim, A. O., Abulfaraj, A. W., & Nagmeldin, W. "Machine learning-based anomaly detection in NFV: A comprehensive survey." *Sensors* 23.11 (2023): 5340.
8. Khalil, U., Malik, O. A., Uddin, M., & Chen, C. L. "A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: a comprehensive review, recent advances, and future research directions." *Sensors* 22.14 (2022): 5168.
9. Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. "A new lightweight cryptographic algorithm for enhancing data security in cloud computing." *Global Transitions Proceedings* 2.1 (2021): 91-99.
10. Antunes, M., Maximiano, M., & Gomes, R. "A client-centered information security and cybersecurity auditing framework." *Applied Sciences* 12.9 (2022): 4102.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Koyeda, V. "Cybersecurity Enhancements for ERP Systems: A Technical Framework." *Sarcouncil Journal of Engineering and Computer Sciences* 4.9 (2025): pp 518-526.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher