Journal of Science, Technology and Social Transformation Volume 2, Issue 02, 2026

A Survey of Zero-Trust Architectures for Artificial Intelligence (AI)-Enabled Payroll ERP Security

Kishankumar Routhu[1*], Krishna Madhav Jha[2], Purna Chandra Rao Chinta[3], Gagan Kumar Patra[4]

Principal Architect, ADP
Manager – Data Management, Topbuild Corp
Sr technical Support Engineer, Microsoft
Data Engineer Specialist, Vanguard

Abstract

AI-based Enterprise Resource Planning (ERP) payroll solutions boost automation, analytics, and operational efficiency but increase the cyber risk surface many times over by centralizing, integrating, and automating processes with clouds. Traditional security perimeter models currently in use are ineffective at protecting such dynamic environments against insider attacks, fraud, and advanced persistent attacks. Zero-Trust Architecture (ZTA) helps address these issues by providing verification, least-privileged access, micro-segmentation, and policy-based enforcement. The author presents the concepts of zero-trust architectures in this survey, which align with AI-enabled payroll ERP security, including key concepts, identity-conscious controls, behavioral analytics, AI-assisted anomaly detection, and context-dependent access controls. The architectural elements, policy orchestration and edge AI methods of continuous authentication and adaptive authorization. It also contrasts the latest studies and models based on AI and Zero Trust used to detect fraud and ensure safe ERP activities.

Keywords: Zero Trust Architecture, AI-enabled ERP, Payroll Security, Fraud Detection, Behavioral Analytics, Adaptive Access Control. DOI: 10.64235/kh9w5a02

Introduction

ERP systems have taken center stage in contemporary organizations, facilitating the integration of key business operations such as human resources, supply chain, finance, and customer service. As organizations move toward digital transformation, ERP platforms are being augmented with artificial intelligence (AI) to automate operations, provide predictive insights, and support data-driven decision-making [1]. Although this transformation enhances operational efficiency, it also increases the attack surface, leaving Enterprise Resource Planning (ERP) ecosystems exposed to sophisticated cyberattacks, unauthorized access, data manipulation, and insider threats. Conventional perimeter-based security models, which are based on fixed trust boundaries, cannot secure dynamic, cloud-based, and AI-enabled ERP systems.

Payroll fraud is a widespread problem in organizations and has resulted in massive financial losses, disrupting operations and damaging their image. The bigger the business, the more complex the payroll system becomes, and it is therefore not economical to have manual oversight of payroll processes; thus, there is always a chance of errors[2] [3]. ERP systems, which are centralized, automated, and integrated with business processes, have been popular for managing payroll functions, but they are susceptible to fraud if not monitored.

The emergence of AI-based ERP solutions creates both opportunities and challenges for the adoption of Zero Trust. On the one hand, AI can optimally increase the ability to monitor in real time, detect anomalies, and predict security[4] The fluid nature of AI processes which operate through interconnected systems creates new challenges for enforcing the established policy[5]. Implementing policy-driven Zero Trust orchestration requires a system that uses real-time evaluation of identity information to manage dynamic authentication policies rather than fixed security rules [6].

ZTA has established itself as a security framework which

Corresponding Author: Kishankumar Routhu Principal Architect, ADP. Email: Kishan1213@gmail.com

How to cite this article: Routhu, K., Jha K.M., Chinta, P.C.R., Patra, G.K. (2026). A Survey of Zero-Trust Architectures for Artificial Intelligence (AI)-Enabled Payroll ERP Security *Journal of Science, Technology and Social Transformation* 2(2), 62-71.

Source of support: Nil

Conflict of interest: None

solves existing security problems by eliminating implicit trust and mandating ongoing user, device, and transaction authentication. In contrast to the notion that network activities are harmless, Zero Trust is predicated on least privilege, micro-segmentation, and real-time risk assessment [7][8]. Nevertheless, supporting Zero Trust in large-scale ERP systems cannot be achieved by relying on authentication or access control policies alone. It requires smart orchestration processes that can understand context, interpret behavior, and automatically adjust security controls in response to an organization's evolving conditions.

Structured of the Paper

The paper has the following structure. Section II illustrates the basics of Zero-Trust architecture. Section III covers AI methods used in payroll ERP security. Section IV discusses the Zero-Trust Architectures of AI-enabled payroll ERP systems. In Section V, a thorough literature review is presented. Lastly, Section VI includes recommendations and directions for future research.

Fundamentals of Zero-Trust Architecture

Zero Trust Architecture (ZTA) establishes security requirements through its core principles and components, providing multiple methods for securing operations based on specific situational contexts and defined security rules and authentication systems [9]but it alsointroduces new security challenges. Traditional perimeter-basedsecurity models are insufficient for cloud environments wherenetwork boundaries are blurred. Zero Trust Architecture (ZTA. The main principles of ZT establish the basic operational structure which organizations need to establish their ZT systems. The core principles can be summarized as follows:

Assume Breach and Implicit Threat

Assume that the environment is already compromised. Every user, device, and network traffic is evaluated as potentially hostile. The organization requires verification of all activities because of this security strategy. The organization establishes no implicit trust for its assets based on their network location or ownership status.

Least Privilege Access

Restrict user and device permissions to just the tasks for which they are created and give no priority to others. The system permits resource access only after individuals submit specific requests that comply with least privilege security requirements. The system assesses trustworthiness through ongoing evaluations because trust does not remain constant.

Continuous Verification

"Always verify" suggests authentication and authorization are not one-time operations. They are continual and dynamic. Each access request is reviewed in real time against contextual parameters (user identification, device posture, location, requested resource, time of day, anomalies, etc.). Session trust may be re-evaluated frequently.

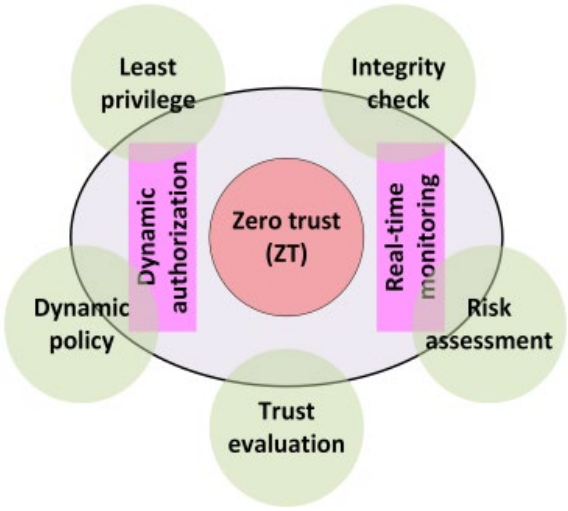

Figure 1: Key Zero-Trust Principles for Information Security in Untrusted Networks.

Secure Every Access and Encrypt Everywhere

All network communications should be secured, regardless of origin or destination. Data must be encrypted both in transit and at rest[10]. Every request from a client to a resource should occur over a secure channel, and preferably through an access proxy or gateway that can enforce policies.

Device and User Authentication

Authenticate and authorize every device and user. Access decisions are based on strong identity verification (such as MFA for users and device identity attestation for devices). Device health or posture (e.g., OS patch level, presence of security agent, etc.) should be checked before granting access

Zero-Trust Security Principles

The fundamental ZT concepts are summarised in Figure. 1 and described below.

Zero Trust

Regardless of where they are placed in the network, all network assets and functions—including devices, computer resources, and services—are treated as untrusted [11]. Hence, all communications must meet the same security standards as those of third parties.

Trust/Risk Evaluation

Every access request is evaluated for risk and trust. The evaluation is conducted both dynamically (depending on current factors) and constantly (during the access time).

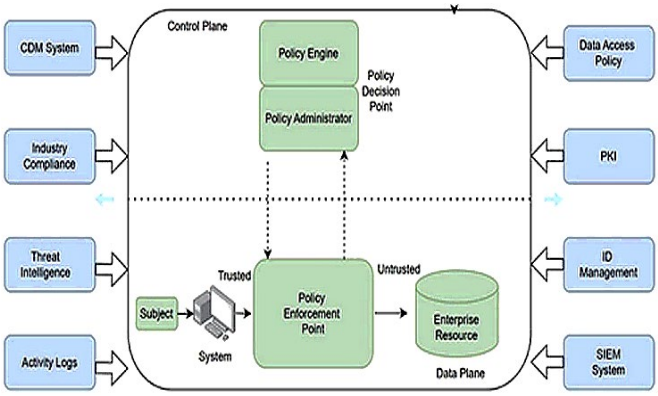

Figure 2: Core Zero Trust Logical Components

Least Privilege

If access is allowed, it should be granted with the least amount of authority. Access is provided solely for a single resource (depending on the resource's sensitivity) and is not valid for any other resource.

Dynamic Policy

To determine whether to allow access, a dynamic policy is required. The essential option factors are the security state (credentials, software versions/patches, location, etc.) and the behavioral features of the subject and network assets.

Integrity Check

All network assets and the requesting subject's security status are continuously monitored, ideally in real time. The automated system assesses compliance with security policy rules by evaluating device security levels, user behavior, and network asset patterns.

Core Components of Zero-Trust Architecture

The framework establishes "never trust, always verify" as its main principle, which necessitates continuous verification of people and devices, combined with their network activity, from a location [12]. Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs) are the fundamental logical elements of the NIST Zero Trust Architecture, as seen in Figure. 2.

Key Components of NIST ZTA

- Policy Enforcement Point (PEP): Implements access determinations by regulating the data transmission among users, devices, and resources.
- Policy Decision Point (PDP): Evaluates access requests according to established policies and variable inputs (e.g., user credentials, device state).
- Identity Provider (IdP): Authenticates and verifies user identities.
- Continuous Diagnostics and Mitigation (CDM): Individual devices and network health and security can be monitored in real time.
- Threat Intelligence and Analytics: provides potential threats and also gives the necessary insight to adjust the policy.
- Data Access Policies: Govern authorization to access resources based on criteria of user roles, device compliance, and risk evaluations.

Identity, Access, and Policy Enforcement

The adoption of Zero-Trust Architectures (ZTA) security policies establishes a fundamental framework for defining access to digital assets. Zero-Trust security systems initiate a trust assessment and maintain a continuous trust evaluation throughout system operation. Policy enforcement is a permanent security system that tracks users' activities, device behavior, and data transfers across different situations [13]. To do this, one needs to develop an elaborate access control policy that uses the user identity, device security status, geographical location, and the resource's protection level as criteria for access permissions.

In the system, a central Policy Decision Point (PDP) enforces security rules, and Policy Enforcement Points (PEPs) authorize network access at various locations. Such a structure guarantees that there is homogeneity in the security controls across all locations where personnel and digital services are provided. Organizations can reduce their security risks by enforcing a Zero-Trust policy, which allows them to grant access only to essential system components. ZTA restricts user and device access to information and systems through the implementation of least-privilege access and micro-segmentation. An HR employee requires specific permission to access financial and engineering systems under this rule.

The rule restricts internal security risks while protecting against security breaches that have already occurred. Dynamic policy enforcement enables immediate access-control changes by analyzing user behavior patterns and suspicious login activity to support real-time decision-making [14]which operates on the principle of \"never trust, always verify,\" has emerged as a foundational security model for cloud environments. However, traditional Zero Trust models, characterized by static policies and rigid access control mechanisms, struggle to keep up with the dynamic nature of modern cloud networks. This review proposes a conceptual shift towards a more granular and dynamic approach to Zero Trust in cloud environments, focusing on the integration of real-time, context-aware access control and adaptive policy enforcement. The new model emphasizes the need for access decisions based on a continuous evaluation of risk, considering factors such as user behavior, device compliance, application context, and environmental conditions. This approach enables more precise, least-privilege access control, ensuring that users and devices only access the resources they need under the right circumstances. By leveraging machine learning, artificial intelligence, and real-time analytics, the

model introduces dynamic policy enforcement that evolves based on ongoing monitoring, rather than relying on static, predefined rules. Furthermore, the review explores the role of identity and access management (IAM. ZT policies use AI and ML to adapt their security measures to changing risk conditions and environmental factors, enhancing an organization's capacity to prevent upcoming security threats.

Payroll Erp Systems And Ai Integration

The integration of AI into payroll ERP systems enables fraud detection, scalability, and real-time monitoring through sophisticated machine learning and behavioral analytics. It further highlights the larger attack surface and new security risks, including data poisoning, model manipulation, and privacy leakage, that require Zero-Trust-based controls across the AI lifecycle.

The artificial intelligence (AI) capability to forecast payroll fraud in Enterprise Resource Planning (ERP) systems can contribute effectively to both the academic literature and the practical business management process, as Figure 3 shows. Organizations need better security solutions, as payroll systems are becoming increasingly complex and fraud schemes are becoming sophisticated, making it difficult to secure financial assets [15]. The key aspects including the following are those where contributes make a lot of contributions in the field:

Advancement of Fraud Detection Methods in ERP Systems

Payroll fraud, a significant issue worldwide, is a scam in which individuals manipulate payroll documents to obtain unauthorized financial gains, resulting in financial losses, operational setbacks, and damage to employee credibility [16]. Conventional fraud detection methods, such as manual auditing and rule-based systems, lack the capacity to process big data and detect sophisticated fraud schemes.

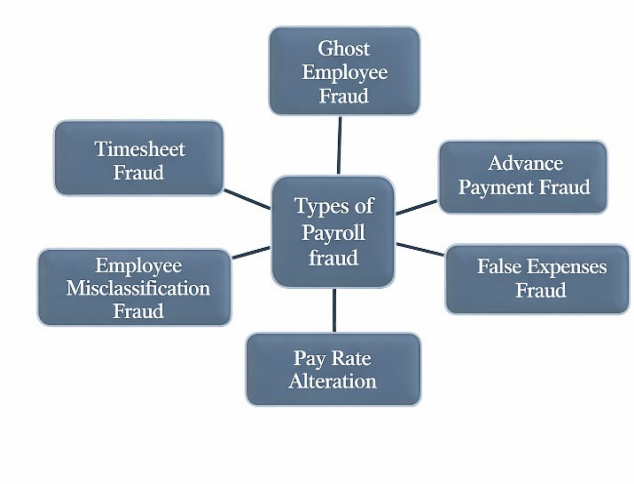

Figure 3: Types of Payroll Fraud

Real-Time Detection and Proactive Fraud Prevention

One of the most necessary contributions is the transition to real-time fraud detection. Traditional fraud detection systems rely on retrospective audits, which investigate the past and thus take a long time to identify fraudulent activities. AI-based fraud detection systems can continuously process payroll information and send timely alerts when they detect abnormal activity patterns [17]. This ability allows the organization to avoid significant financial losses from payroll fraud by acting proactively.

Enhancing Efficiency and Scalability of Fraud Detection

Organizational growth brings on more complex payroll systems, and automated fraud detection is necessary because manual procedures are ineffective. AI systems can handle enormous volumes of data and may scale to meet a company's needs [18]. The system employs ML and DL models that support continuous learning to identify new types of fraud, as existing fraud detection approaches address the scalability issues associated with traditional techniques [19]. Payroll fraud schemes are evolving, yet AI models still detect emerging trends through automated detection algorithms, providing businesses with an effective and scalable solution.

Integration of Unstructured Data Analysis

The primary enhancement is the use of Natural Language Processing (NLP) to manage unstructured data, including emails, internal communications, and transaction approval processes. Textual data contains evidence of fraudulent behavior, such as unauthorized salary increase requests, suspicious communications with employees, and unusual messages about payroll approvals. The use of NLP techniques enables fraud detection to extend beyond structured payroll data, leading to a more thorough investigation of potential fraud risks.

Improving Accuracy and Reducing False Positives

AI models that use ensemble and deep learning as their core technologies achieve better fraud detection results because they can identify authentic transactions with greater precision than standard rule-based systems. The ML techniques DT, SVM, and RF are effective at identifying complex payroll data patterns, leading to improved fraud detection and fewer false positives.

AI-Driven Anomaly and Fraud Detection

A wide variety of AI and ML techniques are used in fraud detection to identify patterns, outliers, and potential fraudulent activity. Data type, intended level of accuracy, and computational efficiency are the determining factors in method selection for fraud detection[20][21]. Here are the

Table1: Summarizing Different Fraud Detection Approaches, Highlighting Their Strengths and Weaknesses

Approach	*Description*	*Strengths*	*Weaknesses*
Supervised Learning Models	Use labeled historical data (fraudulent vs. non-fraudulent) to learn patterns and classify new transactions. Examples: Logistic Regression, Random Forest, SVM.	High accuracy when labeled data is available; well-understood; interpretable in many cases.	Requires large labeled datasets; performance declines with imbalanced data; may not adapt well to new fraud patterns.
Unsupervised & Anomaly Detection Models	Detect anomalies without labeled data by learning normal behavior and flagging deviations. Methods include Autoencoders, Isolation Forests, and Clustering.	Useful when labeled data is scarce; capable of identifying unknown fraud types; adaptive to dynamic environments.	Higher false positive rates; difficult to interpret; may struggle with overlapping fraud and normal patterns.
Reinforcement Learning (RL)	learns the best rules by interacting with the environment through trial and error and adjusting to changing fraud strategies.	Effective in dynamic and adversarial environments; continuously improves with feedback; suitable for real-time detection	Requires careful reward design; computationally intensive; slower convergence; limited adoption in production systems.
Deep Learning & Advanced Architectures	Employ neural networks (ANN, CNN, RNN, LSTM) to capture complex, nonlinear, and high-dimensional fraud patterns from structured and unstructured data.	Handles large-scale and high-dimensional data; captures hidden patterns; can process unstructured data (text, images, etc.).	Requires large datasets and computing power; often a "black box" (low interpretability); risk of overfitting.

main AI and ML techniques used in the most recent cutting-edge research. AI Learning Paradigms are shown in Table I.

Supervised Learning Models

The criminals behind the complex web of financial fraud detection are supervised learning algorithms. Through the careful manipulation of labelled training data, the discovery of patterns, and the perfect orchestration of predictions, their symphony comes to fruition.

Unsupervised and Anomaly Detection Models

Fraud detection methods, like unsupervised anomaly detection, can work even without labelled training data. To identify fraudulent actions, these detection approaches examine out-of-the-ordinary trends in typical transaction behaviour[22]. To do this, the detection methods employ clustering algorithms, autoencoders, and isolation forests. To detect transactions that deviate significantly from expected patterns, autoencoders use neural networks to generate compact representations of typical transaction data.

Reinforcement Learning in Fraud Detection

RL's ability to identify optimal decision policies in dynamic environments has made it a popular choice among researchers as a viable approach to fraud detection. Reinforcement learning is a great fit for monitoring evolving fraud patterns, as it doesn't require supervised learning and instead allows models to learn from their environment.

Deep Learning and Advanced Architectures:

A branch of ML known as DL draws inspiration from ANNs, which mimic how the brain functions. An AI function can learn from unstructured or unlabelled data in a way that mimics how the human brain processes information and generates patterns for decision-making, as shown in Table I:

Behavioral Analytics and User Profiling

Behavioral analytics security solutions rely on interconnected elements that work together to gather, analyze, and evaluate behavioral data. Below, each key component is discussed in depth to show its purpose and technical value in recognizing and prioritizing threats.

Data Collection and Enrichment (Logs, SaaS activity, etc.)

This phase involves collecting unprocessed activity data from several sources, including network traffic flows, endpoint telemetry, authentication logs, and SaaS application events [23]. Collecting high-quality data is essential, as the precision of behavioral analysis relies on the thoroughness and detail of the input. To give the collected events meaning for subsequent modelling and analysis, enrichment adds contextual information, including geolocation, device fingerprinting, and user role metadata.

Behavioral Baseline Modeling

Each individual, device, or entity's typical behaviour is defined through behavioural baseline modelling, based on past behaviour over time. To improve accuracy, the sophisticated models can separate baselines by peer groups (e.g., engineering team vs. finance team). This is usually done using techniques such as clustering algorithms or probabilistic models to distinguish legitimate variability from possible anomalies, providing a basis for valid anomaly detection.

Anomaly Detection Engines

The anomaly detection engine, which compares real-time activity against predefined baselines to identify anomalies that may indicate danger, is the central component of behavioral analytics systems. These types of engines combine statistical thresholds, unsupervised ML (k-means, DBSCAN, or autoencoders), and, in certain instances, supervised models of known attack patterns. Good engines evolve to minimize false hits, making them sensitive to changing patterns while remaining sensitive to true anomalies.

Risk Scoring and Prioritization

Anomalies are not equally threatening. Risk scoring assigns risk to identified abnormalities based on factors such as asset sensitivity, user privilege levels, and threat intelligence feeds. Prioritization frameworks ensure that security teams focus on the highest-impact occurrences first, allowing more efficient incident response and resource allocation [24]. To enhance risk forecasts, sophisticated systems may employ Bayesian inference or weighted scoring models.

Security Implications of AI-Driven Payroll Systems

Artificial intelligence implemented in payroll systems can improve automation, precision, and decision-making, but it also creates complex security issues. AI-generated payroll systems rely heavily on large volumes of confidential employee information, including payroll data, tax information, and individual identifiers, which increases the overall security risk of the system [25]. The use of data-driven models, data pipelines, APIs, and third-party integrations exposes the system to unauthorized access, data breaches, and system exploitation [26]. Furthermore, the ongoing data feeding of models to train and infer new data introduces new vulnerabilities for adversaries to feed malicious inputs or exploit vulnerabilities in the data validation mechanism [27]. AI-based payroll systems are vulnerable to model manipulation and data poisoning attacks. Opponents can manipulate training data or corrupted input streams to bias their model predictions, causing them to calculate payroll incorrectly, make fraudulent payouts, or even violate compliance.

Zero-Trust Architectures for Ai-Enabled Payroll Erp

Application of the Zero Trust Architecture (ZTA) in ERP systems requires a systematic implementation strategy that ensures continuous validation, secure data management, and adaptive access control at every level of operation. Defense organizations that use ZTA are focusing on building a secure-by-design ERP configuration that can recognize and control hazards in real time.

Identity and Access Management (IAM)

ZTA is based on the correct validation of identities. Adaptive authentication measures, such as multi-factor authentication (MFA), device posture, and behavioral analytics, are used to verify ERP users [28]. Every access request is authenticated against user role, device condition and context such as time, location and mission sensitivity. Such dynamic IAM architecture does not allow the blanket trust but rather implements continuous verification on the lifecycle of the session.

Micro-Segmentation and Least-Privilege Access

ERP modules are categorized into operational units such as logistics, intelligence, finance, and maintenance. Micro-segmentation is done to ensure a user or a device entering a domain is not automatically laterally transferred into another domain. The independent access controls and encrypted communication channels protect each segment and curb the transmission of threats.

Continuous Monitoring and AI-Driven Threat Detection

Artificial intelligence is very important in the contemporary ZTA-based ERP context. Real-time analytics constantly analyzes network traffic, identifies anomalies, and attempts to compromise. The machine learning models are used to compare user behavior with historical baselines to enable adaptive control, e.g., terminating sessions, re-authenticating, or quarantining compromised endpoints.

Cloud-Native Deployment and Policy Enforcement

In a world where defense ERP systems are moving to hybrid and cloud environments, policy enforcement should be applied uniformly across all infrastructure. The access security controls offered by cloud-native systems, including Secure Access Service Edge (SASE) and Identity Governance models, are used to counter unified access monitoring. Policies are automatically synchronized between cloud and on-premises ERP modules, ensuring continuity of operations without compromising the security posture.

Integration with Defense Communication Networks

ZTA implementation should align with current classified network systems, such as the Defense Information Systems Network (DISN). Interoperability is provided with encrypted gateways and federated identity management systems, without involving confidentiality. Adherence to military-grade encryption and auditor logs of all data access and exchange activities makes tracing any such activity possible.

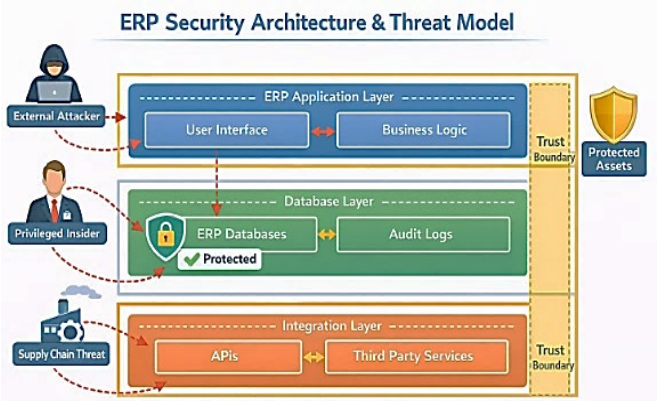

Figure 4: ERP Security Architecture and Threat Model Illustrating Trust Boundaries and Adversary Vectors

Edge Integration of Zero-Trust with ERP Systems

ERP System Components and Attack Surface. Figure 4 presents an integrated ERP security architecture with a detailed threat model that illustrates how various adversaries interact with ERP components across trust boundaries. The architecture is further broken down into three main layers: the ERP application layer, the database layer, and the integration layer [29]. Every layer corresponds to a specific domain of security where there are certain assets, access routes and profile risks. The boundaries of trust are clearly displayed to highlight where security controls should be implemented to prevent unauthorized access and lateral movement.

End users interact with the system at the application layer, with the user interface and business logic modules as the main components. External attackers exploit this tier by targeting open-ended interfaces, such as web doorways and application access points, and frequently use weak authentication, session hijacking, or input validation vulnerabilities [30]. The two-way traffic between business logic and the user interface illustrates how compromised front-end access can spread deeper into ERP processes unless it is properly secured by ongoing verification and access-control systems.

The database tier is the central repository for confidential ERP data, including financial records, personnel data, and transactional data. The trustees of privileged insiders are explicitly depicted to be a significant danger at this tier because of the valid access privileges, which can be exploited to distort or steal data[31]fast, and eliciting linear growth. Typical approaches to handling Payroll and time management experience various problems, particularly scalability, error-prone, and ineffectiveness. The innovation under discussion is called "Smart HR", the machine learning-based concept for combining payroll procedures and optimizing the human capital's working time. This system uses supervised learning approaches for making payroll fraud and error prediction, learning for grouping workforce patterns, and reinforcement learning for scheduling. The hybrid approach has important advantages as it concerns time-saving, cost reduction and accuracy. It is an innovative module incorporating the ability to analyze employee work and attendance patterns and the prior payroll cycles. Furthermore, there is an option for a Time Optimization Module (TOM. The auditing log underscores the importance of monitoring and forensic visibility. In contrast, the encrypted database icon underscores the importance of encryption, access control, and behavioral analytics to protect the most important assets.

The integration layer identifies risks posed by APIs and third-party services, which are becoming a growing concern in contemporary ERP ecosystems. Supply chain threats are illustrated entering through external integrations, emphasizing how compromised vendors or insecure APIs can bypass traditional perimeter defenses[32]. The presence of trust boundaries across layers aligns with Zero-Trust principles, demonstrating that no component or user is implicitly trusted. Overall, the figure effectively conveys the need for AI-driven monitoring and Zero-Trust enforcement across all ERP layers to ensure robust, end-to-end security.

Edge AI-Driven Continuous Authentication

Behavioral biometrics relies on modelling complex and sometimes delicate patterns in human behaviour. Conventional statistical methods have been replaced by AI methods, which are much better at learning temporal and spatial relationships in behavioral data (see Figure 5). Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) are most commonly used for tasks such as Typing Dynamics, Motion Sensors, Behavioral Biometrics, Touchscreen Gestures, and Mouse Movement. Formers can model sequential dependencies (i.e., sequences of actions to be performed (symbols to be typed) or the sequence of individual steps in a gait).

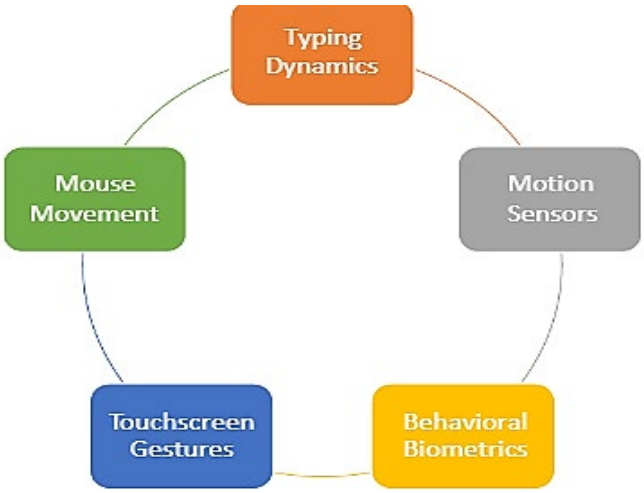

Figure 5: Conceptual Diagram of Behavioral Biometrics Modalities

Table2 : Comparative Analysis of Related Works on Zero-Trust and AI-Enabled ERP Security

Authors (Year)	*Focus Area*	*Key Findings*	*Approaches*	*Future Work*
Andrew and Espy et al., (2026)	Zero-Trust Data Governance for AI Systems	Establishes zero-trust as a continuous, intelligence-driven governance model for AI	Zero-trust across AI data lifecycle using trust scoring and policy automation	Empirical validation, real-world deployment, and integration with operational AI platforms
Paul et al., (2025)	Policy-Driven Zero Trust in AI-Enabled ERP	Dynamic policy enforcement with AI analytics improves assurance, access control, and threat detection	Policy-driven orchestration with identity-centric verification and ML-based anomaly detection	Scalability analysis, performance optimization, and ERP–cloud integration
Saurabh et al., (2025)	AI-Enhanced Zero-Trust Enterprise Architecture	AI/ML strengthen zero-trust through real-time risk assessment and adaptive access control	AI-based architecture with IAM, micro-segmentation, policy enforcement, and behavioral analytics	Architecture standardization, cross-cloud interoperability, and long-term studies
Barbosa et al., (2024)	AI-Driven Zero Trust for ERP Systems	AI with zero-trust enables real-time security automation while preserving privacy	ML-based behavioral analytics and adaptive access control in Oracle ERP	Extension to non-Oracle ERP platforms and large-scale workload evaluation
Bhat et al., (2023)	AI-Based Threat Detection in Zero-Trust ERP	Behavioral analytics with zero-trust improves detection accuracy and reduces false positives	ML/DL models for continuous authentication, least privilege, and micro-segmentation	Advanced sequential models, cross-module correlation, and response automation
Bibi and Jan et al., (2022)	Unified AI and Zero Trust for Critical Infrastructure	AI–zero trust integration enhances resilience, detection, and response	Unified system with predictive analysis, anomaly detection, and automated response	Explainable AI, real-world deployment, and long-term trust evaluation

The other commonly used models, such as a DT and RM, provide more interpretable classification with good accuracy and low training cost, and thus are very appealing to lightweight authentication systems[33]. The Hidden Markov Model (HMM) has successfully modelled the sequential changes in behavioral attributes. Transformer-based architectures have recently demonstrated the potential to combine data from multiple sensors, achieving state-of-the-art performance in continuous authentication tasks.

Context-Aware and Adaptive Access Control

Context-Based Access Control (CBAC) is an advanced security mechanism that restricts access to digital resources based on the context of an access request. In contrast to typical systems that depend on set, predetermined rules, CBAC dynamically examines risk variables such as:

- User location (office, remote, unusual geography)
- Device type and health (corporate laptop vs. personal phone, patched vs. unpatched)
- IP address and network trust
- Time of request (regular business hours vs. unusual times)
- User role and permissions

If the context aligns with predefined secure conditions, access is granted. If not, additional verification may be required (multi-factor authentication), or access may be denied outright[34]the proliferation of the Internet of Things (IoT. This contextual authentication helps ensure only the right users, under the right conditions, gain entry.

CBAC is a variation of static access control models, such as Role-Based Access Control (RBAC), that adds real-time checks. It is an essential building block of ZT systems, in which there is no implicit trust in devices, users, and sessions.

Literature Review

The implementation of AI-based Zero-Trust designs is gaining momentum in the literature reviewed, with a focus on securing ERP and AI-oriented environments. As shown in Table II. Past studies have focused on sustained verification, access control policy, behavior analytics, and automated threat detection, which collectively can improve resilience, data integrity, and reliability in a multifaceted, dynamic, and adversarial business environment.

Andrew and Espy et al. (2026) present a conceptual and architectural construct of zero-trust data governance customized to AI-centric settings, characterized by relentless learning, fluid data flows, and sustained adversarial pressure. It discusses the aspects of operationalization of zero-trust principles throughout the data lifecycle, including its acquisition and pre-processing to model training, inference, and feedback loops. This article offers a fundamental insight into protecting AI-driven cyber ecosystems by reframing data governance as an active, intelligence-led control system rather than a functional compliance capability [35].

Paul et al. (2025) note that Enterprise Resource Planning (ERP) systems have become highly interconnected, AI-driven applications that support an organization's core operations. These systems are getting more complex, and traditional security patterns that are based on perimeters cannot

be trusted to avert advanced cyber threats, insider risks, and breaches of data integrity. It discusses a policy-based ZT orchestration system designed to enhance ongoing assurance in AI-driven ERP systems. The paper identifies how real-time monitoring, access control, and risk-based authentication, together with dynamic policy enforcement, identity-centric verification, and AI-driven analytics, can improve one another [36].

Saurabh et al. (2025) Zero-Trust Architecture (ZTA) has also emerged as a paradigm of security in response to this evolving threat environment, grounded in constant verification, least-privilege access, and clear trust assessment. The design and implementation of a ZT, AI-enhanced enterprise architecture, and work in hybrid and multi-cloud environments are discussed, with references to both strategic planning and actual implementation. The article discusses how AI and ML can enhance ZT by providing real-time risk assessment, behavioral analytics, adaptive access control, and automated threat detection [37].

Barbosa et al. (2024) report that Enterprise Resource Planning (ERP) systems have become essential to business operations today, but their centralized nature makes them prime targets for cyberattacks. It proposes an AI-based framework that integrates privacy-conscious schemes with ZT designs to automate cybersecurity for Oracle-based ERP systems in real time. Using ML and behavioral analytics, the framework constantly scans system activity, identifies anomalies, and enforces adaptive access control without interrupting business processes [38].

Bhat et al., (2023) ERP security architecture that integrates AI-driven threat detection and ZT security framework. To identify unusual and harmful activity early, ML and DL models are used to analyse user behaviour, transaction patterns, and system data in real time. The framework can detect more precisely with less false positives by using behavioral analytics and sequential modeling. The principles of a ZT also enhance security through continuous authentication, identity-based access controls, least-privilege enforcement, and micro-segmentation between ERP modules [39].

Bibi et al. (2022) argue that an integrated solution that incorporates artificial intelligence (AI) and Zero Trust (ZT) concepts can serve as a revolutionary solution to these problems. ZT features an identity verification, stringent access control, and continuous monitoring philosophy that outlines the principle of never trust, always verify to prevent unauthorised access and lateral movement. This model is even stronger when combined with AI. The ZT framework is enhanced by AI-powered real-time anomaly detection, predictive threat assessments, and automated responses, enabling more adaptive and intelligent security measures [40]often reliant on perimeter defenses, fail to adequately safeguard these vital systems against advanced attacks. A unified approach integrating artificial intelligence (AI.

Conclusion And Future Work

The role of the Zero-Trust Architecture (ZTA) as a protective instrument for an AI-enabled Payroll ERP system is to help mitigate the expanding attack surface as automation, data centralization, and cloud integration increase. These dynamic environments cannot be addressed with traditional perimeter-based security; instead, continual validation, least-privilege access, micro-segmentation, and policy-based enforcement should be used. The research mentioned the benefits of applying AI-based methods to enhance Zero-Trust controls, including anomaly detection, behavioral analytics, and adaptive risk scoring, which enable fraud detection and real-time contextual access decisions. The main ZTA elements, identity-based controls, edge AI-based continuous authentication, and context-specific authorization models were discussed in relation to the current research. According to the literature, the combination of AI and Zero Trust enhances the accuracy of detection, resiliency, and operational assurance of payroll ERP ecosystems. Altogether, AI-based Zero-Trust systems are scalable, intelligent platforms for securing sensitive payroll processes against evolving cyber threats and insider risks.

Further studies are needed on the real-world application and performance of AI-assisted Zero-Trust payroll ERP systems, lightweight edge-based authentication schemes, explainable AI for security decision-making, and cross-cloud policy coordination. There are also standards and benchmarks for payroll fraud and ERP threat modelling, along with datasets used to validate and compare solutions.

References

[1] A. Efe, "Risk Modelling of Cyber Threats Against MIS and ERP Applications," *Pamukkale Üniversitesi İşletme Araştırmaları Derg.*, vol. 11, no. 2, pp. 502–530, Dec. 2024, doi: 10.47097/piar.1550812.

[2] B. Chen, "The Comprehensive Evolution of ERP Systems: Classification, Financial Integration, and Future AI Integration," *Int. J. Artif. Intell. Mach. Learn.*, vol. 5, no. 2, July, pp. 51–65, 2025, doi: 10.51483/IJAIML.5.2.2025.51-65.

[3] A. Parupalli, "The Evolution of Financial Decision Support Systems : From BI Dashboards to Predictive Analytics," *KOS J. Bus. Manag.*, vol. 1, no. 1, pp. 1–8, 2023.

[4] D. Ajish, "The significance of artificial intelligence in zero trust technologies: a comprehensive," *J. Electr. Syst. Inf. Technol.*, vol. 11, no. 1, Aug, pp. 01-23, 2024, doi: 10.1186/s43067-024-00155-z.

[5] A. Parupalli, "Business Intelligence in ERP ML-Based Comparative Study for Financial Forecasting," *ESP Int. J. Commun. Eng. Electron. Technol.*, vol. 2, no. 4, pp. 17–26, 2024, doi: 10.56472/25839217/IJCEET-V2I4P103.

[6] M. Osaka and S. Lawrence, "Zero-Trust Data Governance with AI-Driven Access Management," *Int. J. Adv. Eng. Technol. Innov.*, vol. 02, no. 01, May, pp. 821–839, 2024.

[7] B. Saha and P. Goel, "Leveraging AI to Predict Payroll Fraud in Enterprise Resource Planning (ERP) Systems," *SSRN Electron. J.*, vol. 11, pp. 2284–2304, 2023, doi: 10.2139/ssrn.5224746.

[8] G. Maddali, "Zero Trust Security Architectures for Large-Scale Cloud Workloads," *Int. J. Res. Anal. Rev.*, vol. 5, no. 2, pp. 960–965, 2018.

[9] Y. Akharchaf, "Zero Trust Architecture in Cloud Security: Challenges and Implementation," 2025. doi: 10.13140/RG.2.2.26671.04000.

[10] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.

[11] K. Ramezanpour and J. Jagannath, "Intelligent Zero Trust Architecture for 5G/6G Tactical Networks: Principles, Challenges, and the Role of Machine Learning," 2021. doi: 10.48550/arXiv.2105.01478.

[12] G. Mehta *et al.*, "Emerging Cybersecurity Architectures and Methodologies for Modern Threat Landscapes," vol. 5, pp. 28–40, 2024, doi: 10.5281/zenodo.14275106.

[13] A. Khan, P. Sharma, and K. Qureshi, "Policy Enforcement and Authentication Strategies in Zero-Trust Architectures," 2017. doi: 10.13140/RG.2.2.27124.46721.

[14] C. C. Ike and A. B. Ige, "Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement," *Magna Sci. Adv. Res. Rev.*, vol. 2, no. 1, pp. 074–086, Jun. 2021, doi: 10.30574/msarr.2021.2.1.0032.

[15] S. Enokkaren, R. Kendyala, J. Kurma, J. V. Mamidala, V. Bitkuri, and A. Attipalli, "Artificial Intelligence (AI)-Based Advance Models for Proactive Payroll Fraud Detection and Prevention," 2024, doi: 10.63665/ijmlaidse.

[16] A. K. Meshram, "Real-Time Financial Fraud Prediction Using Big Data Streaming on Cloud Platforms," *Int. J. Res. Publ. Eng. Technol. Manag.*, vol. 8, no. 5, 2025, doi: 10.15662/IJRPETM.2025.0805021.

[17] A. Parupalli, "Business-Oriented Employee Performance Assessment via Machine Learning in ERP Systems," *TIJER – Int. Res. J.*, vol. 11, no. 11, 2024.

[18] J. Bhat, D. Sundar, and Y. Jayaram, "Modernizing Legacy ERP Systems with AI and Machine Learning in the Public Sector," *Int. J. Emerg. Res. Eng. Technol.*, vol. 3, no. 4, pp. 104–114, 2022.

[19] S. A. Pushkala, "Financial Fraud Identification Using Graph Neural Network And LSTM With Autoencoder-Based Data Refinement," *J. Int. Cris. Risk Commun. Res.*, vol. 9, no. 1, 2026.

[20] U. I. Okoli, O. C. Obi, A. O. Adewusi, and T. O. Abrahams, "Machine learning in cybersecurity: A review of threat detection and defense mechanisms," *World J. Adv. Res. Rev.*, vol. 21, no. 1, pp. 2286–2295, 2024.

[21] S. Thangavel, S. Srinivasan, S. B. V. Naga, and K. Narukulla, "Distributed Machine Learning for Big Data Analytics: Challenges, Architectures, and Optimizations," *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 4, no. 3, pp. 18–30, Oct. 2023, doi: 10.63282/3050-9262.IJAIDSML-V4I3P103.

[22] G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," vol. 4, no. 3, pp. 209–218, 2024, doi: 10.56472/25832646/JETA-V4I3P122.

[23] [23] M. Kanwal, N. A. Khan, and A. A. Khan, "A Machine Learning Approach to User Profiling for Data Annotation of Online Behavior.," *Comput. Mater. \& Contin.*, vol. 78, no. 2, 2024.

[24] A. G. Martín, A. Fernández-Isabel, I. M. de Diego, and M. Beltrán, "A survey for user behavior analysis based on machine learning techniques: current models and applications," *Appl. Intell.*, vol. 51, no. 8, january, pp. 6029–6055, 2021, doi: 10.1007/s10489-020-02160-x.

[25] R. Korrapati, "AI-Driven Transformation of Payroll Management: Enhancing Efficiency, Accuracy, and Compliance," 2023. doi: 10.2139/ssrn.5131030.

[26] V. Verma, "Security Compliance and Risk Management in AI-Driven Financial Transactions," *Int. J. Eng. Sci. Math.*, vol. 12, no. 7, July, pp. 107–121, 2023.

[27] A. Bamiduro, "AI driving payroll management systems: A multi-case study analysis," *World J. Adv. Res. Rev.*, vol. 28, no. 2, pp. 2065–2072, 2025, doi: 10.30574/wjarr.2025.28.2.3900.

[28] A. L. Paul, "Zero-Trust Architecture in ERP Systems: Strengthening Cyber Resilience in National Defense Infrastructure," 2025.

[29] P. Chandrashekar and M. Kari, "Design Machine Learning-Based Zero-Trust Intrusion Identification Models for Securing Cloud Computing System," *Int. J. Res. Anal. Rev.*, vol. 11, no. 4, pp. 901–907, 2024.

[30] A. Dalal, S. Abdul, and F. Mahjabeen, "Ensuring ERP Security in Edge Computing Deployments: Challenges and Innovations for SAP Systems," *SSRN Electron. J.*, 2025, doi: 10.2139/ssrn.5248376.

[31] J. R. Vummadi, H. Volikatla, and S. Dodda, "Smart HR for Smart Enterprises: A Machine Learning-Based Approach to Payroll Automation and Time Optimization," *Int. J. Artif. Intell. Data Sci. Mach. Learn.*, vol. 6, no. 3, pp. 80–89, 2025, doi: 10.63282/3050-9262.IJAIDSML-V6I3P113.

[32] A. Gupta, "A Strategic approach - Enterprise-Wide Cyber Security Quantification via Standardized Questionnaires and Risk Modeling impacting financial sectors globally," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 3, no. 1, Mar. 2022, doi: 10.63282/3050-9416.IJAIBDCMS-V3I1P110.

[33] U. Ejaz, P. Panchal, S. A. M. Islam, and A. Imashev, "Behaviour Biometrics Using AI for Continuous Authentication Systems," *J. Artif. Intell. Gen. Sci. ISSN3006-4023*, vol. 8, pp. 53–64, 2025, doi: 10.60087/jaigs.v8i02.386.

[34] A. S. M. Kayes *et al.*, "A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues," *Sensors*, vol. 20, no. 9, 2020, doi: 10.3390/s20092464.

[35] J. Andrew and L. Espy, "Towards Zero-Trust Data Governance In Ai-Driven Cyber Ecosystems," 2026.

[36] A. L. Paul, "Policy-Driven Zero Trust Orchestration in AI- Enabled ERP for Continuous Assurance," 2025.

[37] K. Saurabh, "Design and Execution of a Zero-Trust, AI-Enabled Enterprise Architecture Across Hybrid and Multi-Cloud Infrastructure," 2025.

[38] A. L. Barbosa, "AI-Driven Privacy and Zero-Trust Architectures in ERP: Real-Time Cybersecurity Automation for Oracle-Based Enterprises," *Int. J. Adv. Res. Comput. Sci. \& Technol.*, vol. 7, no. 3, pp. 10313–10317, 2024.

[39] J. Bhat, "Strengthening ERP Security with AI-Driven Threat Detection and Zero-Trust Principles," *Int. J. Emerg. Trends Comput. Sci. Inf. Technol.*, vol. 4, pp. 154–163, 2023, doi: 10.63282/3050-9246.IJETCSIT-V4I3P116.

[40] S. Bibi and I. Jan, "AI and Zero Trust: A Unified Approach to Securing Critical Infrastructure," 2022. doi: 10.13140/RG.2.2.15804.14724.