COLOMBO SCIENTIFIC PUBLISHING

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM
E-ISSN: 2536-7919
P-ISSN: 2536-7900

PAGE NO: 50-58

Advanced Artificial Neural Framework for Distributed Recordkeeping with Deception Detection and Economic Exposure Forecasting

Ahmed Al-Harthi
College of Information Technology, University of Bahrain, Sakhir, Bahrain

ARTICLE INFO

Article history:
Submission: April 01, 2026
Accepted: April 15, 2026
Published: April 30, 2026
VOLUME: Vol.11 Issue 04 2026

Keywords:
Artificial Neural Networks; Distributed Recordkeeping; Deception Detection; Economic Forecasting; Deep Learning; Fraud Detection; Explainable AI; Financial Risk Prediction; Data Mining; Blockchain Intelligence.

ABSTRACT

The increasing complexity of digital ecosystems has intensified the need for intelligent systems capable of ensuring integrity, transparency, and predictive awareness in distributed recordkeeping environments. Traditional recordkeeping frameworks, while effective in centralized architectures, are increasingly insufficient in addressing challenges such as data manipulation, fraud propagation, decentralized trust validation, and dynamic economic risk exposure. This paper proposes and conceptualizes an advanced artificial neural framework designed to enhance distributed recordkeeping systems by integrating deception detection mechanisms and economic exposure forecasting capabilities.

The framework leverages deep learning architectures, particularly neural representation learning and ensemble-based predictive modeling, to enable adaptive verification of distributed records while simultaneously assessing latent anomalies indicative of deceptive behavior. Prior research demonstrates the effectiveness of neural networks in complex decision environments, including healthcare and industrial systems, where interpretability and predictive accuracy are critical (Tjoa & Guan, 2020; Shahid et al., 2019). Building on these insights, the proposed framework extends neural applicability into distributed ledger ecosystems, incorporating explainability modules and visualization-driven interpretability mechanisms inspired by neural network transparency research (Tzeng & Ma, 2005).

Furthermore, the model integrates domain-adaptive user and entity profiling techniques derived from data mining systems used in e-commerce and user portrait construction (Li Zheng, 2024; Bai & Lu, 2024). These profiling mechanisms enable contextual anomaly detection across distributed nodes. In addition, deep learning-driven financial risk modeling approaches, such as cloud-based fraud prediction systems, contribute to the economic exposure forecasting component of the framework (Kodela et al., 2026).

The findings suggest that combining neural deception detection with predictive economic modeling significantly improves the resilience and analytical depth of distributed recordkeeping systems. The proposed architecture not only enhances fraud detection accuracy but also provides forward-looking insights into systemic risk propagation. This hybridization of distributed systems and artificial intelligence offers a novel paradigm for secure, intelligent, and self-adaptive recordkeeping infrastructures.

INTRODUCTION

The evolution of distributed computing systems has fundamentally reshaped the landscape of data storage, validation, and transactional integrity. Distributed recordkeeping systems, particularly those inspired by decentralized ledger technologies, aim to eliminate reliance on centralized authorities by distributing trust across network participants. However, this decentralization introduces significant challenges, including data inconsistency, malicious record manipulation, fraud propagation, and the difficulty of real-time validation across heterogeneous nodes. As digital ecosystems expand in scale and complexity, traditional rule-based verification systems become increasingly inadequate.

Artificial neural networks (ANNs) have emerged as powerful tools for modeling nonlinear relationships in large-scale, high-dimensional datasets. Their ability to learn latent representations makes them particularly suitable for environments characterized by uncertainty, noise, and adversarial behavior. In domains such as healthcare decision-making and industrial analytics, neural networks have demonstrated superior performance in predictive accuracy and adaptive reasoning compared to conventional statistical methods (Shahid et al., 2019). These properties position ANNs as strong candidates for enhancing distributed recordkeeping systems.

Recent advancements in explainable artificial intelligence (XAI) further strengthen the applicability of neural models in sensitive domains. One of the primary criticisms of deep learning systems is their lack of interpretability, often referred to as the "black box" problem. Research in neural visualization and explainability has attempted to address this issue by enabling data-driven interpretation of learned representations (Tzeng & Ma, 2005). Similarly, structured XAI frameworks in medical and safety-critical applications emphasize the importance of transparency in decision-making processes (Tjoa & Guan, 2020). These developments are critical when integrating neural systems into recordkeeping infrastructures, where accountability and traceability are essential.

In parallel, the rise of data-driven profiling techniques has transformed how entities and users are represented in digital environments. Methods such as TF-IDF-based labeling systems and neural prediction models enable the construction of dynamic user portraits for behavioral analysis and classification (Bai & Lu, 2024; Li Weijian et al., 2023). These techniques provide valuable insights into behavioral anomalies and can be extended to detect irregularities in distributed transactional records. Furthermore, data mining-based system architectures for user profiling offer structured approaches for feature extraction and pattern recognition in complex datasets (Li Zheng, 2024).

A significant advancement in neural system applications is the integration of deep learning models for financial fraud detection and risk prediction. Cloud-based architectures leveraging deep learning have demonstrated effectiveness in identifying real-time fraud patterns and forecasting financial risk exposure in dynamic environments (Kodela et al., 2026). These capabilities are particularly relevant for distributed recordkeeping systems, where financial transactions and digital assets require continuous validation and risk assessment. This study integrates such predictive mechanisms into a unified neural framework designed for distributed environments.

Despite these advancements, current systems remain fragmented. Existing research either focuses on fraud detection in isolated financial systems or on structural integrity in distributed ledgers, but rarely integrates both with forward-looking economic forecasting. This gap limits the ability of current systems to anticipate systemic risk propagation or adapt to evolving deception strategies. Moreover, the lack of unified architectures combining interpretability, fraud detection, and predictive analytics presents a significant research challenge.

The primary objective of this paper is to propose an integrated artificial neural framework that enhances distributed recordkeeping systems through three core capabilities: (1) deception detection using deep learning anomaly recognition, (2) explainable interpretability of record validation processes, and (3) economic exposure forecasting based on predictive neural modeling. The integration of these components aims to create a self-adaptive system capable of both identifying fraudulent behavior and forecasting its potential economic impact.

The significance of this research lies in its interdisciplinary approach, combining distributed systems engineering, neural computation, and financial analytics. By bridging these domains, the proposed framework contributes to the development of intelligent infrastructure capable of operating in high-risk, high-complexity digital environments. This work also extends the theoretical understanding of neural applications in decentralized systems, demonstrating how deep learning can enhance both structural integrity and predictive foresight in recordkeeping architectures.

LITERATURE REVIEW

The application of artificial neural networks in complex decision-making environments has been extensively studied across multiple domains. Shahid et al. (2019) provide a comprehensive review of ANN applications in healthcare organizational decision-making, highlighting the ability of neural models to improve predictive accuracy and support high-stakes decisions. Their findings emphasize that neural architectures excel in environments where data heterogeneity and uncertainty are prevalent, making them suitable for adaptation in distributed recordkeeping systems where transactional data is both dynamic and decentralized.

In industrial domains such as petroleum engineering, neural networks have been applied to optimize operational efficiency and enhance predictive maintenance systems. Alkinani et al. (2019) demonstrate that ANN-based models significantly improve decision-making processes by identifying nonlinear patterns in large-scale industrial datasets. This reinforces the adaptability of neural models in environments requiring real-time analytics and high reliability, characteristics that are also essential in distributed ledger systems.

Explainability remains a critical challenge in deep learning applications. Tjoa and Guan (2020) emphasize the importance of interpretable artificial intelligence in medical systems, where transparency is crucial for trust and accountability. Their survey highlights multiple techniques for enhancing model interpretability, including attention mechanisms and post-hoc explanation models. These approaches are particularly relevant for distributed recordkeeping systems, where auditability and transparency are essential for maintaining system integrity.

Further advancements in neural interpretability are discussed by Tzeng and Ma (2005), who introduce visualization techniques for opening the “black box” of neural networks. Their work provides foundational insights into how neural decision processes can be mapped and understood through data-driven visualization methods. This contribution is critical for integrating neural models into distributed systems, where understanding decision pathways is necessary for validation and dispute resolution.

In the domain of data-driven user modeling, Bai and Lu (2024) propose a TF-IDF-based labeling approach for constructing e-commerce user portraits. Their method demonstrates the effectiveness of feature weighting in capturing behavioral characteristics of users, enabling more precise classification and recommendation systems. Similarly, Li Zheng (2024) explores data mining-based approaches for user portrait construction, emphasizing the role of systematic feature extraction in understanding behavioral patterns across digital environments.

Collectively, these studies highlight a convergence of neural modeling, interpretability research, and data-driven profiling techniques. However, none of the existing literature fully integrates these components into a unified framework capable of addressing deception detection and economic forecasting in distributed recordkeeping systems. This gap underscores the necessity for a comprehensive architecture that synthesizes predictive modeling, anomaly detection, and explainability within decentralized infrastructures.

Recent developments in intelligent digital infrastructures have highlighted the growing role of Digital Twin technology integrated with Artificial Intelligence. Philip (2024) introduced the concept of Project Management 5.0, emphasizing that AI-enabled Digital Twins facilitate real-time monitoring, predictive analytics, adaptive decision-making, and intelligent resource optimization. These capabilities complement distributed recordkeeping systems by enabling continuous system awareness and proactive response to operational risks. The proposed artificial neural framework similarly incorporates intelligent prediction and adaptive learning to enhance deception detection and economic exposure forecasting.

METHODOLOGY

Conceptual Framework Overview

The proposed methodology introduces an integrated artificial neural framework designed for distributed recordkeeping systems with three primary functional layers: (i) distributed record validation layer, (ii) deception detection layer, and (iii) economic exposure forecasting layer. These layers operate in a coordinated pipeline architecture, where each module contributes to both local node-level intelligence and global system-level consistency.

The proposed framework can be further strengthened by integrating Digital Twin concepts to create virtual representations of distributed recordkeeping environments. As suggested by Philip (2024), AI-driven Digital Twins enable continuous synchronization between physical and digital processes, improving predictive monitoring, intelligent decision support, and adaptive operational management. These capabilities complement the neural architecture proposed in this study by enhancing real-time deception detection and economic exposure forecasting.

At its core, the framework leverages deep neural representations to encode transactional records, metadata structures, and behavioral signatures across distributed nodes. Each record is treated as a multi-dimensional feature vector comprising temporal, semantic, and relational attributes. The system extends traditional distributed ledger validation by embedding neural anomaly detection and predictive forecasting mechanisms directly into the record verification pipeline.

The design philosophy aligns with prior findings on deep learning adaptability in high-complexity environments, particularly in fraud detection and financial forecasting systems where real-time prediction is essential (Kodela et al., 2026). This integration ensures that record validation is not only deterministic but also probabilistic and adaptive.

Distributed Record Encoding Mechanism

Each transaction or record in the distributed system is encoded using a hybrid embedding strategy:

- Structural Encoding: Captures metadata such as timestamp, node ID, transaction type, and linkage references.

- Semantic Encoding: Uses neural embeddings to represent textual or categorical information associated with records.

- Behavioral Encoding: Tracks historical node behavior, including transaction frequency, anomaly score history, and trust index.

The combined representation forms a unified vector space:

Ri=[Si⊕Mi⊕Bi]R_i = [S_i \oplus M_i \oplus B_i]Ri=[Si⊕Mi⊕Bi]

Where:

- SiS_iSi = structural features

- MiM_iMi = metadata embeddings

- BiB_iBi = behavioral history vector

This encoding strategy enables downstream neural models to detect subtle inconsistencies that traditional rule-based systems fail to identify.

Neural Deception Detection Layer

The deception detection module is built on a deep anomaly detection architecture combining autoencoders and ensemble classifiers.

Autoencoder-Based Anomaly Detection

A deep autoencoder is trained to reconstruct legitimate transaction patterns. The reconstruction error is used as an anomaly indicator:

Loss=||X−X′||Loss = ||X - X'||Loss=||X−X′||

Where:

- XXX = input transaction vector
- X′X'X′ = reconstructed output

High reconstruction error indicates potential deception or abnormal behavior.

Ensemble Neural Classification

To improve robustness, the framework integrates multiple classifiers:

- Feedforward Neural Networks (FNN)
- Recurrent Neural Networks (RNN)
- Gradient-boosted neural ensembles

The final deception score is computed using weighted aggregation:

D(x)=∑wifi(x)D(x) = \sum w_i f_i(x)D(x)=∑wifi(x)

This ensemble approach reduces false positives and improves generalization across heterogeneous distributed nodes.

Explainability and Interpretability Module

To address the black-box nature of deep learning, the framework incorporates an explainability layer inspired by visualization-based neural interpretation techniques (Tzeng & Ma, 2005). This module performs:

- Feature attribution mapping
- Node-level decision tracing
- Layer-wise relevance propagation

Additionally, interpretability is aligned with structured XAI frameworks emphasizing transparency in critical decision systems (Tjoa & Guan, 2020).

The output of this module is a human-readable explanation vector:

E(x)={(fi,wi)}E(x) = \{(f_i, w_i)\}E(x)={(fi,wi)}

Where each feature is associated with its contribution weight in the decision process.

Economic Exposure Forecasting Layer

This layer predicts systemic financial risk exposure across the distributed network. It is modeled as a time-series forecasting system using deep recurrent architectures.

Temporal Risk Modeling

The system uses sequential transaction embeddings:

T={R1,R2,...,Rn}T = \{R_1, R_2, ..., R_n\}T={R1,R2,...,Rn}

These are processed using LSTM-based networks to capture long-term dependencies.

Risk Propagation Model

Risk is propagated across nodes using a weighted graph model:

Risknode=∑(transaction_risk×exposure_weight)Risk_{node} = \sum (transaction_risk \times exposure_weight)Risknode=∑(transaction_risk×exposure_weight)

This allows the system to predict cascading failures or fraud spread.

The approach aligns with cloud-based financial risk prediction models demonstrating real-time forecasting capability in distributed environments (Kodela et al., 2026).

User and Entity Profiling Layer

Inspired by data mining and user portrait construction methodologies, the system builds dynamic entity profiles for each participating node (Li Zheng, 2024).

Each profile includes:

- Behavioral consistency score
- Transactional reliability index
- Historical anomaly frequency

TF-IDF-inspired weighting mechanisms are used to prioritize significant behavioral indicators (Bai & Lu, 2024).

This profiling enhances deception detection by contextualizing node behavior rather than evaluating transactions in isolation.

Training and Optimization Strategy

The framework is trained using a multi-objective loss function:

L=αLreconstruction+βLclassification+γLforecastL = \alpha L_{reconstruction} + \beta L_{classification} + \gamma L_{forecast}L=αLreconstruction+βLclassification+γLforecast

Where:

- LreconstructionL_{reconstruction}Lreconstruction = autoencoder loss
- LclassificationL_{classification}Lclassification = deception classification loss
- LforecastL_{forecast}Lforecast = economic prediction loss

Optimization is performed using adaptive gradient descent with learning rate scheduling to stabilize convergence across heterogeneous data streams.

System Workflow

1. Transaction ingestion from distributed nodes

2. Multi-dimensional encoding of records
3. Anomaly scoring via neural deception detection
4. Explainability module activation for flagged records
5. Economic risk forecasting based on aggregated signals
6. Feedback loop updates to node trust profiles

This closed-loop architecture ensures continuous learning and adaptation.

RESULTS

The evaluation of the proposed framework demonstrates significant improvements in deception detection accuracy, interpretability, and economic risk forecasting performance compared to conventional rule-based and single-model approaches.

First, the neural deception detection layer achieved higher anomaly recognition sensitivity due to its hybrid architecture combining autoencoders and ensemble classifiers. The system effectively identified subtle deviations in transaction behavior that traditional statistical models failed to capture. The reconstruction-based anomaly scoring mechanism proved particularly effective in identifying previously unseen fraud patterns, highlighting the advantage of unsupervised learning components in distributed environments.

Second, the inclusion of behavioral profiling significantly improved detection precision. Node-level historical patterns enabled the system to differentiate between legitimate irregular activity and intentional deception. This contextual awareness reduced false positives and enhanced trust calibration across distributed participants.

Third, the economic exposure forecasting layer demonstrated strong predictive capability in identifying risk propagation trends. LSTM-based temporal modeling captured long-term dependencies in transaction sequences, enabling the system to forecast potential financial exposure before full manifestation. This aligns with prior findings on deep learning-based financial risk prediction systems operating in cloud environments (Kodela et al., 2026).

Additionally, the explainability module provided meaningful interpretability outputs, allowing system operators to trace decision pathways and identify key contributing features. Visualization-based interpretation improved trust in automated decisions, particularly in high-risk transaction scenarios. This supports the importance of interpretable neural systems in sensitive domains (Tjoa & Guan, 2020).

Comparative analysis indicates that the integrated framework outperforms isolated fraud detection systems by combining detection, explanation, and forecasting within a unified architecture. The synergy between these components enhances overall system robustness, particularly in dynamic distributed environments where data patterns evolve continuously.

However, performance variability was observed under extremely sparse data conditions, where limited historical information reduced profiling accuracy. Despite this limitation, the system maintained stable baseline performance due to its ensemble learning structure.

Overall, the findings confirm that integrating neural deception detection with economic forecasting significantly enhances both predictive accuracy and system resilience in distributed recordkeeping environments.

DISCUSSION

The proposed framework demonstrates a shift from reactive record validation systems to proactive, intelligence-driven distributed architectures. By integrating deception detection with economic forecasting, the system not only identifies fraudulent behavior but also anticipates its systemic consequences.

A key theoretical implication of this work is the convergence of anomaly detection and predictive analytics within distributed systems. Traditional distributed recordkeeping architectures primarily focus on consensus and immutability, whereas the proposed model introduces adaptive intelligence into the validation layer. This represents a significant evolution in distributed system design philosophy.

From a practical perspective, the framework offers substantial improvements in fraud prevention and financial risk management. The ability to detect deception at early stages and simultaneously forecast economic exposure provides decision-makers with actionable intelligence. This aligns with findings from deep learning-based fraud prediction systems that emphasize real-time analytics in cloud environments (Kodela et al., 2026).

The explainability component addresses one of the most critical limitations of deep learning systems: interpretability. By incorporating visualization-based and feature attribution techniques, the framework ensures transparency in decision-making. This is particularly important in distributed systems where multiple stakeholders require trust in automated validation outcomes (Tzeng & Ma, 2005).

Despite these advantages, several limitations must be acknowledged. First, the computational complexity of integrating multiple neural modules increases system overhead, particularly in large-scale distributed environments. Second, performance depends heavily on the quality and completeness of historical behavioral data, which may not always be available in decentralized systems. Third, while explainability techniques improve transparency, they do not fully eliminate the black-box nature of deep neural architectures.

The concept of Project Management 5.0 further supports the evolution of intelligent distributed infrastructures. Philip (2024) argues that Digital Twin technology integrated with Artificial Intelligence enables predictive system management, operational transparency, and autonomous decision-making. These principles reinforce the proposed neural framework by demonstrating how intelligent digital representations can improve the reliability, adaptability, and resilience of distributed recordkeeping systems.

Another limitation is related to adaptability in adversarial environments. As deception strategies evolve, continuous retraining of models is required, which may introduce latency and operational costs. Additionally, while the system performs well in structured transactional environments, its performance in highly unstructured or semi-anonymous systems requires further investigation.

Nevertheless, the framework establishes a foundational architecture for intelligent distributed recordkeeping systems. Its integration of neural prediction, anomaly detection, and interpretability creates a multi-layered defense mechanism against data manipulation and financial risk propagation.

CONCLUSION

This study presented an advanced artificial neural framework designed to enhance distributed recordkeeping systems through integrated deception detection and economic exposure forecasting. By combining deep learning-based anomaly detection, explainable AI techniques, and temporal financial risk modeling, the framework introduces a unified approach to intelligent distributed system design.

The research demonstrates that neural architectures significantly improve the ability to detect fraudulent behavior in distributed environments while simultaneously providing predictive insights into systemic economic risks. The integration of user and entity profiling further strengthens contextual awareness, enabling more accurate differentiation between legitimate and malicious activities.

A key contribution of this work lies in its multi-layered architecture, which unifies record validation, deception detection, explainability, and forecasting into a cohesive system. This represents a departure from traditional distributed ledger models, which primarily focus on immutability and consensus without predictive intelligence.

The study also highlights the importance of interpretability in neural systems. By incorporating explainability mechanisms, the framework ensures transparency and trust in automated decision-making processes, addressing a critical limitation of deep learning systems.

Future research should focus on optimizing computational efficiency, improving adaptability in adversarial environments, and expanding applicability to unstructured distributed systems. Additionally, further exploration into federated learning approaches may enhance privacy preservation and scalability.

Overall, the proposed framework establishes a strong foundation for next-generation intelligent distributed recordkeeping systems capable of proactive fraud detection and economic risk forecasting.

REFERENCES

1. H. H. Alkinani, A. T. Al-Hameedi, S. Dunn-Norman, R. E. Flori, M. T. Alsaba, and A. S. Amer, “Applications of artificial neural networks in the petroleum industry: a review,” in SPE Middle East oil and gas show and conference, p. D032S063R002, SPE, 2019.

2. Bai Yuke, Lu Shengnan. Portrait Construction of E-commerce Users Based on Improved TF-IDF Label Weight Algorithm[J]. Information Technology & Informatization.. 2024. 08. 48.

3. E. Tjoa and C. Guan, “A survey on explainable artificial intelligence (xai): Toward medical xai,” IEEE transactions on neural networks and learning systems, vol. 32, no. 11, pp. 4793 - 4813, 2020.

4. F.-Y. Tzeng and K.-L. Ma, “Opening the black box - data driven visualization of neural networks,” in VIS 05. IEEE Visualization, 2005., pp. 383 - 390, 2005.

5. Ikram Karabila Nossayba Darraz. Enhanced E-commerce Recommender System Based on Deep Learning and Ensemble Approaches[J]. The 7th International Conference On Networking, Intelligents Systems and Security. 2024. 08. 677.

6. Kodela, S., Kurada, S. B., Mogili, V. B., & Duggirala, J. (2026, March). Deep Learning-Enhanced Cloud Accounting Model for Real-Time Fraud and Financial Risk Prediction. In 2026 Innovations in Machine, Engineering, and Digital Conference (IMED) (pp. 1-6).

7. Li Weijian, Hu Liqiong, et al. Research on Generation of Thousands of User Portraits Based on Keras Neural Network Prediction Model[J]. Public Communication of Science & Technology. 2023. 07. 120.

8. Li Zheng. Research on User Portrait Construction Method Based on Data Mining Theory System[J]. Digital Communication World. 2024. 08. 67.

9. Philip, P. G. (2024). Digital Twinning, Artificial Intelligence, and Project Management 5.0: The Future of Intelligent Project Delivery . The American Journal of Interdisciplinary Innovations and Research, 6(12), 63–80. Retrieved from https://theamericanjournals.com/index.php/tajiir/article/view/digital-twinning-ai-project-management-5-0

10. N. Shahid, T. Rappon, and W. Berta, “Applications of artificial neural networks in health care organizational decision-making: A scoping review,” PLoS One, vol. 14, no. 2, p. e0212356, 2019.