CIA Open Access

Revolutionizing Management with AI and Blockchain for Smarter Anomaly Detection and Fraud Prevention

Noiralih Guere Castellanos
MSc in Customs and International Trade
Corresponding Email Id: noiralih@email.com

DOI: 10.63575/CIA.2023.10102

Abstract

In today's rapidly evolving digital landscape, businesses and financial institutions face increasingly sophisticated fraudulent activities, cyber threats, and operational anomalies. Traditional rule-based fraud detection methods often fail to counter these evolving threats effectively. This article explores the integration of Artificial Intelligence (AI) and Blockchain technology as a revolutionary approach to fraud detection and anomaly prevention in dynamic management systems. AI-driven models, including machine learning, deep learning, and predictive analytics, play a crucial role in identifying fraudulent patterns in real-time. The proposed framework employs advanced AI techniques such as tree-based models (Random Forest, XGBoost), deep learning architectures (autoencoders, fully connected neural networks), and sequential models (LSTM, GRU) to enhance fraud detection capabilities. Additionally, statistical methods, including the Five Number Summary, Z-Score Analysis, and Chi-Square Tests, further refine anomaly detection by identifying deviations in transaction behaviors. Blockchain technology reinforces security through its decentralized, tamper-resistant ledger, preventing unauthorized data alterations and ensuring transparent auditing. By integrating AI and Blockchain, this framework enhances fraud detection accuracy, minimizes false positives, and strengthens risk management. This synergy offers a comprehensive, intelligent, and secure solution for modern financial and business management systems, effectively safeguarding operations against evolving fraud tactics.

Keywords: *Dynamic Management Systems, Random Forest, XGBoost, LSTM, GRU, Z-Score Analysis, Chi-Square Tests*

Introduction

In today's digital era, businesses and financial institutions are facing an increasing wave of fraud, cyber threats, and operational anomalies that can lead to financial losses, reputational damage, and regulatory penalties. Traditional fraud detection and management systems, which rely on predefined rule-based algorithms and manual auditing, often fall short in detecting sophisticated fraud tactics such as identity theft, transaction manipulation, money laundering, and insider fraud [1]. As cybercriminals adopt more advanced techniques, organizations require intelligent, real-time, and tamper-proof mechanisms to safeguard their operations. The integration of **Artificial Intelligence (AI)** and **Blockchain** is emerging as a revolutionary solution to enhance anomaly detection and fraud prevention in management. AI brings machine learning, deep learning, and predictive analytics to identify fraudulent patterns, while Blockchain ensures **data integrity, transparency**, and **immutability**. The synergy between these two technologies enables **real-time fraud detection, secure transaction processing,** and **decentralized risk management**, reducing human intervention and improving decision-making [2][3]. Figure 1 visualizes the comparison of Fraud detection approach in management system.

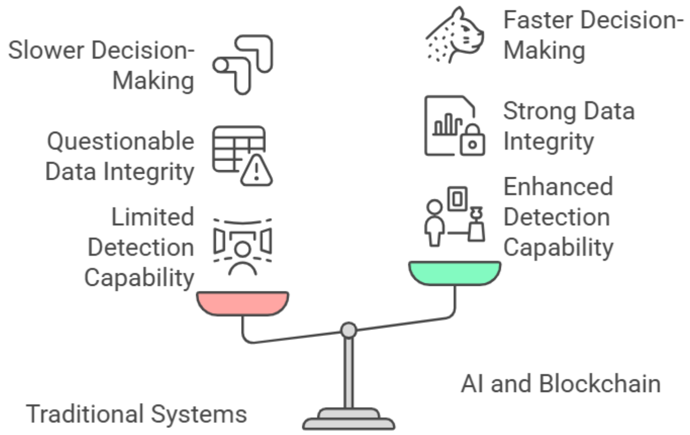

Figure 1: Comparison of Fraud Detection Approach

Fraudsters are continuously evolving their methods to bypass traditional security measures, making it increasingly difficult for businesses to detect and prevent fraudulent activities. The complexity and scale of fraud have expanded with the rise of digital transactions and the global interconnectedness of businesses. Common fraudulent activities in management include **credit card and payment fraud**, where criminals use stolen financial information to make unauthorized transactions, and **identity theft**, in which fraudsters impersonate legitimate users to gain unauthorized access to sensitive data. **Supply chain fraud** involves the manipulation of procurement processes, such as fake invoices, misrepresentation of product authenticity, and counterfeiting, while **insider fraud** refers to employees exploiting system vulnerabilities for financial gain or to cause data breaches. Traditional rule-based fraud detection models, although widely employed, often fall short in identifying **unknown** or **evolving fraudulent patterns**. These models typically rely on predefined rules or thresholds, which can miss novel forms of fraud or generate **false positives** that lead to inefficiencies. Figure 2 visualizes the challenges in the fraud detection [4][5]. In this article, we will discuss the detailed techniques and algorithms that can be used for fraud detection, including **statistical methods** such as **Five Numbers Theory, tree-based algorithms**, and **sequential models** such as **Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU),** and others in detecting financial anomalies.

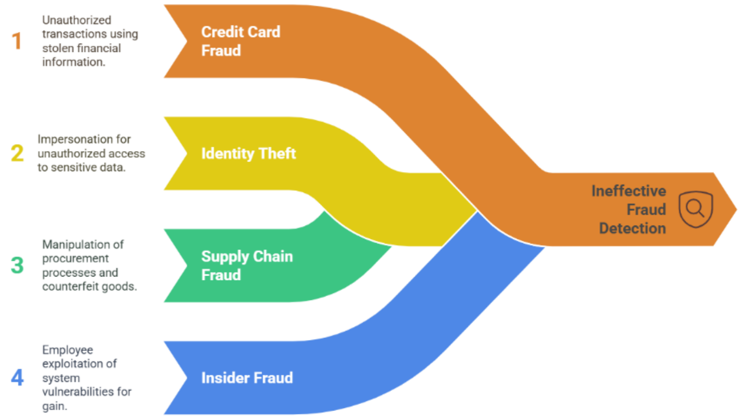
1
Unauthorized transactions using stolen financial information.
Credit Card Fraud
2
Impersonation for unauthorized access to sensitive data.
Identity Theft
3
Manipulation of procurement processes and counterfeit goods.
Supply Chain Fraud
4
Employee exploitation of system vulnerabilities for gain.
Insider Fraud
Ineffective Fraud Detection

Figure 2: Challenges in Fraud Detection

Methodology

The methodology for anomaly detection and fraud prevention in management leverages a combination of **Artificial Intelligence (AI), Blockchain Technology**, and advanced **statistical and machine learning techniques. Figure 3** visualizes this methodology, illustrating how AI and Blockchain collaborate in fraud prevention and detection within management systems. In the following section, we will provide a detailed discussion of these components and their integration.

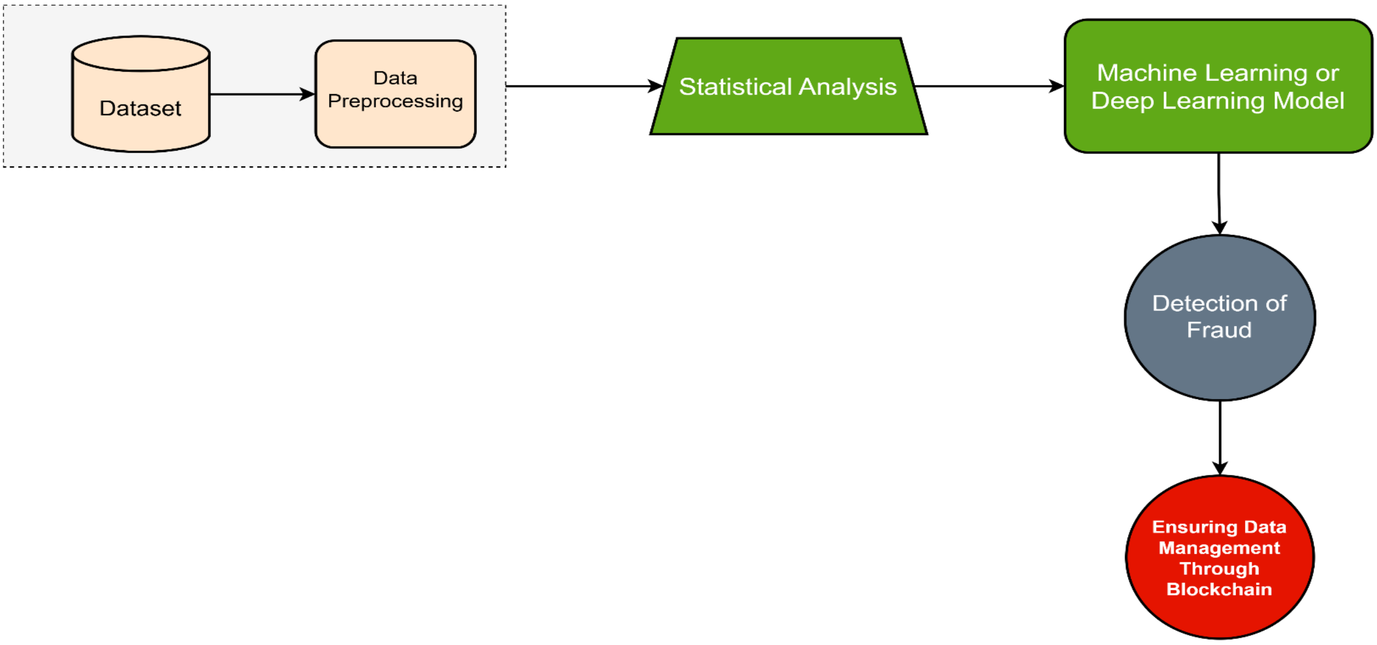
Dataset
Data Preprocessing
Statistical Analysis
Machine Learning or Deep Learning Model
Detection of Fraud
Ensuring Data Management Through Blockchain

Figure 3: Methodology of Fraud Detection and Management with AI and Block chain

I. Data Collection and Preprocessing:

Fraud detection heavily relies on **high-quality, structured, and tamper-proof data**. The data preprocessing steps are crucial for transforming raw data into a clean and structured format that can be efficiently used for **machine learning** and **AI models**. The data preprocessing steps are crucial for transforming raw data into a clean and structured format that can be efficiently used for **machine learning** and **AI models**. Below are the key preprocessing steps involved in preparing the dataset for anomaly detection:

Data Cleaning: The first step in preprocessing is **data cleaning**, where any **missing, incomplete**, or **inconsistent** values in the dataset are identified and removed or corrected. This step ensures that the models are not affected by data noise, which could lead to inaccurate predictions. Common issues addressed during data cleaning include missing transaction details, duplicate records, and erroneous entries [6].

Feature Engineering: Feature engineering involves the extraction of meaningful and relevant features from the raw data. In fraud detection, important features could include **transaction frequency**, **transaction amount**, **location of transaction, time patterns, user behaviors,** and **historical transaction data**. For example, if a user typically makes transactions in a certain location, a sudden transaction from a geographically distant location could raise a flag for potential fraud. Similarly, unusual spikes in transaction amounts or frequency could indicate suspicious activity [7].

Normalization and Standardization: Once the features are extracted, the next step is to normalize and standardize the data to ensure that different features are on a similar scale. This is important for machine learning models, as features with larger numerical values might dominate the learning process and skew results. **Normalization** ensures that all numerical data is transformed into a uniform range, typically between **[0,1] [8].** This is done using **Min-Max Scaling**, which scales each feature by subtracting the minimum value and dividing by the range (maximum value minus minimum value). Mathematically, for a given feature x_i, the **normalized value** x_i' is calculated as:

$$x_i' = \frac{x_i - \min(X)}{\max(X) - \min(X)}$$

Anomaly Labeling: The next step involves **anomaly labeling**. For supervised machine learning models, it is essential to label historical data as either **fraudulent** or **non-fraudulent**. This process is critical because it provides the model with the necessary information to learn patterns of fraudulent and legitimate behavior. By labeling a portion of the data, the model can train on **labeled examples**, and then generalize to detect anomalies in new, unseen data [9]. Mathematically, this step can be represented by a vector X of **transaction features**, where:

$$X = [\, x_1, x_2, x_3, x_4, x_5 \dots\dots\dots\dots\dots\ x_n]$$

II. Statistical Analysis:

Statistical analysis plays a crucial role in identifying anomalies and outliers in financial transactions, which are often indicative of fraudulent activities. In the context of fraud detection, statistical methods are used to model the normal behavior of transactions and identify deviations from this norm. The goal is to capture patterns in the data and detect outliers, which could be indicative of fraud. Popular technique such as five number summary, Z-Score Analysis discussed here.

Five Number Summary: The Five Numbers Summary is a statistical method used to summarize the distribution of a dataset and is especially useful in detecting potential fraud. It consists of five key values: the minimum (the smallest value), the first quartile (Q_1) (25th percentile), the median (Q_2) (50th percentile), the third quartile (Q_3) (75th percentile), and the maximum (the largest value) [10]. From these values, the Interquartile Range (IQR) is calculated by the following ways:

$$IQR = Q_3 - Q_1$$

The IQR shows where the middle 50% of the data lies. Any transaction falling outside the range $Q_1 - 1.5 \times IQR$ or $Q_3 + 1.5 \times IQR$ is flagged as an outlier and considered an anomaly, which might indicate fraudulent activity.

Z Score Analysis: Its also a statistical method used to detect anomalies by measuring how far a transaction deviates from the mean of a dataset in terms of standard deviations [11]. It is calculated as:

$$Z = \frac{x_i - \mu}{\sigma}$$

Where x_i is the transaction value, μ is the mean and σ is the standard deviation. A Z-score greater than 3 or less than -3 indicates that the transaction is significantly different from the normal pattern and may be flagged as fraudulent.

Chi-Square Test: It is used to compare the observed and expected frequencies of transactions in different categories [12]. It is calculated as:

$$X^2 = \sum \frac{(O_i - E_i)}{E_i}$$

Where O_i is the observed frequency and $\boldsymbol{E_i}$ is the expected frequency. If the Chi-Square value exceeds a certain threshold, it suggests a significant difference between observed and expected patterns, potentially indicating fraudulent activity. This test is particularly useful for analyzing categorical transaction data and uncovering hidden fraud patterns. Figure 4 shows the outliers of the transactions, which generally count as anomaly or fraudulent transactions.

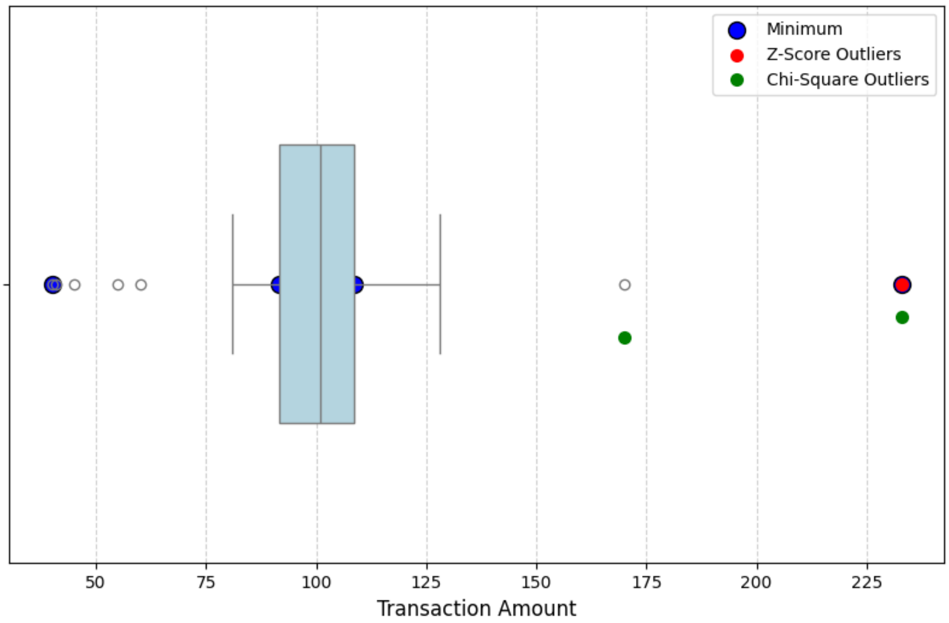

Figure 4: Anomaly Detection with Statistical Techniques

III. Fraud Detection using AI-based Models:

AI-driven models have revolutionized fraud detection by enabling real-time anomaly detection, pattern recognition, and predictive analytics. Unlike traditional rule-based systems, AI-based models can dynamically learn from data, adapt to evolving fraud tactics, and reduce false positives. The key AI techniques used in fraud detection include tree-based models, deep learning architectures, and sequential models.

a. Tree Based Models:

Tree-based machine learning models, such as Random Forest and XGBoost, are widely used for fraud detection due to their ability to handle structured financial data efficiently. These models classify transactions based on multiple decision trees, where each tree contributes to the final fraud prediction. Given a transaction $X = [x_1, x_2, x_3, x_4 \dots \dots \dots \dots\ x_n]$ tree-based models iteratively split the data based on feature importance (e.g., transaction amount, frequency, location) to maximize classification accuracy. The model assigns a probability score to each transaction, where a high probability indicates potential fraud [13]. Figure 5 visualizes the Tree based models fraud detection process.

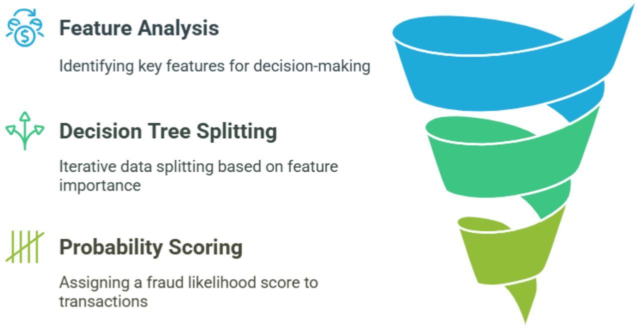
Feature Analysis
Identifying key features for decision-making
Decision Tree Splitting
Iterative data splitting based on feature importance
Probability Scoring
Assigning a fraud likelihood score to transactions

Figure 5: Tree Based Models Fraud Detection Process

b. Deep Learning Models:

Deep learning models, such as autoencoders and fully connected neural networks (FCNNs), are highly effective in detecting fraud patterns in high-dimensional data. Autoencoders are unsupervised models trained to reconstruct normal transactions; deviations from reconstruction indicate anomalies [14]. Mathematically, an autoencoder compresses input X into a lower-dimensional representation Z and reconstructs it as $\widehat{x}$, where anomalies result in high reconstruction errors:

$$Reconstruction\ Error = \ \|x - \hat{x}\|^2$$

A high error score suggests fraudulent activity. Figure 6 visualizes the basic auto encoder architecture.

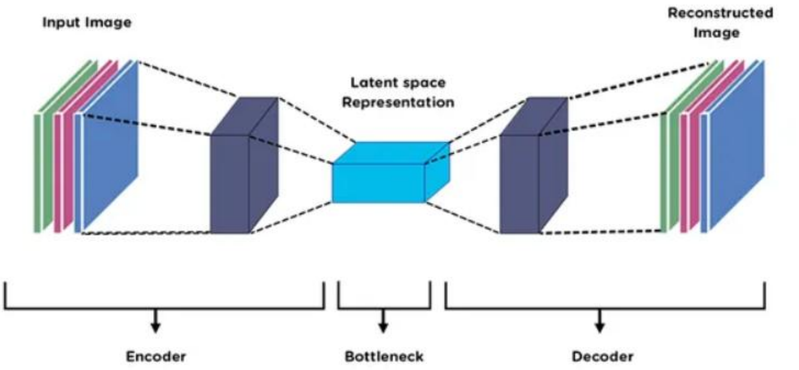

Figure 6: Auto Encoder Architecture [14]

c. Sequential Models:

Fraudulent activities often exhibit sequential patterns over time, where a single suspicious transaction may not always indicate fraud, but a pattern of abnormal behavior over multiple transactions can reveal fraudulent intent. This makes sequential modeling techniques such as Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU) highly effective in detecting fraud based on time-series transaction data [15]. These models are particularly useful in analyzing user behavior, detecting anomalies in payment histories, and identifying unusual spending patterns. Traditional fraud detection systems often analyze transactions independently, treating each one as an isolated event. However, fraudulent behaviors tend to evolve over time, requiring a model that can detect patterns within a sequence of events. LSTM and GRU models are specialized types of Recurrent Neural Networks (RNNs) designed to retain memory of past transactions and use this information to predict whether a new transaction is likely to be fraudulent. They take in a sequence of transactions, analyze the relationships between them, and determine whether the pattern deviates from normal behavior. Mathematically, we represent a sequence of transactions as:

$$T = [t_1, t_2, t_3, \dots\dots\dots\dots\ t_n]$$

Where t_i represents a transaction at time step i.

Long Short Term Memory(LSTM) for fraud detection:

LSTMs address the limitations of standard RNNs, which struggle with long-term dependencies due to the vanishing gradient problem [16]. LSTM networks incorporate memory cells that selectively retain or forget information over long sequences. This makes them ideal for fraud detection, where fraudulent behaviors may unfold gradually over multiple transactions. At each time step t the LSTM updates its hidden state h_t using the following equations:

Forget Gate: Decides how much past information should be retained or discarded

$$f_t = \ \sigma(W_f. [h_{t-1}, x_t] + \ b_f)$$

Input Gate: Determines how much new information should be added to the memory

$$i_t = \ \sigma(W_i. [h_{t-1}, x_t] + \ b_i)$$

Cell State Update: Updates the memory cell with new candidate values

$$\tilde{c}_t = \ tanh(W_c. [h_{t-1}, x_t] + \ b_c)$$
$$c_t = \ f_t \ \times C_{t-1} + \ i_t \ \times \ \tilde{c}_t$$

Output Gate: Decides what part of the memory should be sent to the next layer

$$O_t = \sigma(W_o . [h_{t-1}, x_t] + b_o)$$
$$h_t = O_t \times \tanh(C_t)$$

By maintaining long-term memory of transaction sequences, LSTMs can detect gradual shifts in user behavior, such as slowly increasing transaction amounts, unusual geographic locations, or abnormal time gaps between purchases. If the hidden state h_t deviates significantly from expected patterns, the transaction is flagged as potentially fraudulent. Figure 7 visualizes the architecture of LSTM, illustrating its gating mechanism and key characteristics

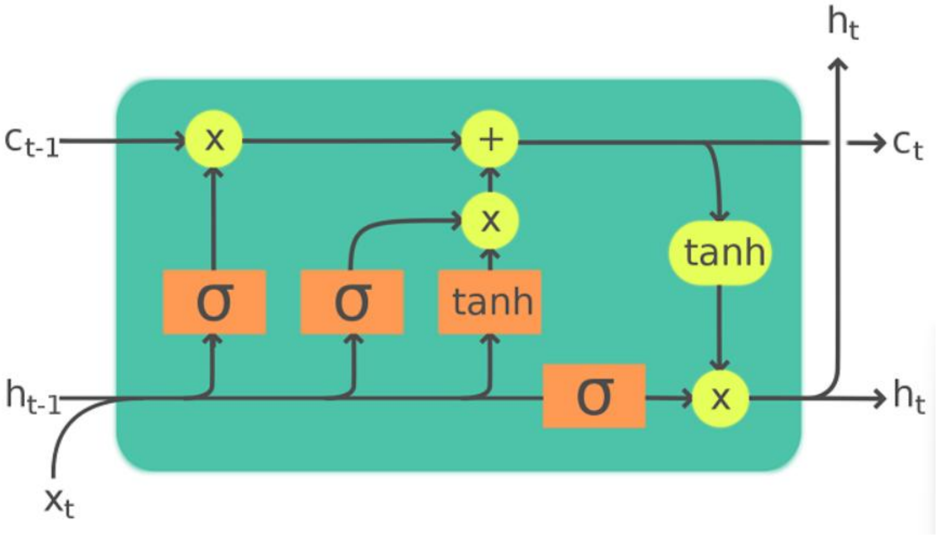

Figure 7 : Architecture of LSTM [17]

Blockchain for Secure and Transparent Data Management

Blockchain technology plays a crucial role in ensuring secure, immutable, and transparent data management in fraud detection systems. Traditional databases are vulnerable to manipulation, unauthorized access, and central points of failure, making them less reliable for fraud prevention [18]. In contrast, blockchain provides a decentralized, tamper-proof, and auditable ledger, enhancing the integrity of financial transactions and management systems. Figure 8 illustrates blockchain technology's contribution to fraud detection systems. The following section discusses three key components of this technology in detail.

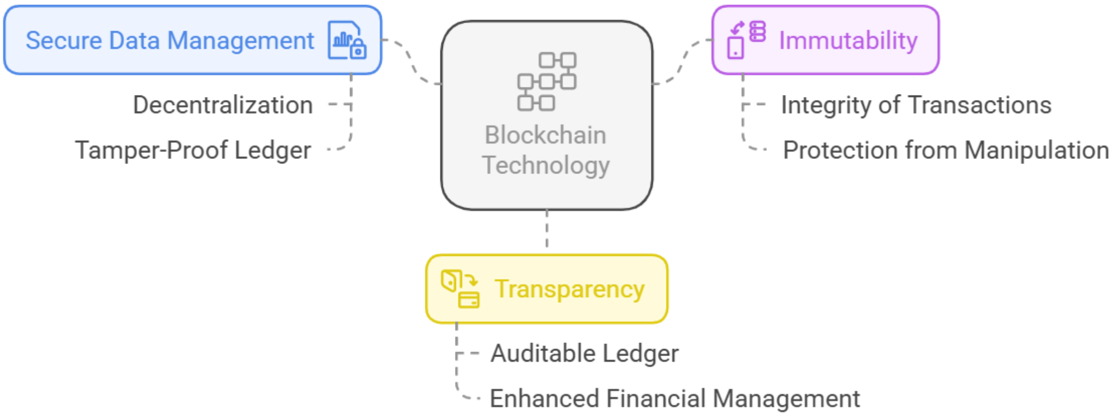

Figure 8: Block Chain Technology in Fraud Detection

I. Decentralization and Tamper Resistance:

Blockchain operates on a distributed network of nodes where each transaction is recorded in a block and linked cryptographically to the previous block, forming an immutable chain. This ensures that once a transaction is recorded, it cannot be altered or deleted, preventing fraudsters from manipulating financial records. Blockchain technology operates on a distributed network of nodes, ensuring that no single entity has complete control over the data. Each transaction is recorded in a block, which is then cryptographically linked to the previous block, forming a chain of immutable records. This structure prevents unauthorized modifications, ensuring data integrity and security in fraud prevention systems. Unlike traditional centralized databases, which are vulnerable to hacking, insider threats, and data corruption, blockchain's decentralized nature eliminates single points of failure. Each block in the blockchain contains a unique hash, which is generated using cryptographic hashing algorithms like SHA-256. This hash serves as a fingerprint for the block, and any change in transaction data alters the hash value, making fraud easily detectable [19]. The hash of a block is computed as:

$$H = hash(T, H_{prev}, nonce)$$

Where T represents the transaction data, $\boldsymbol{H_{prev}}$ is the hash of the previous block, and **nonce** is a variable adjusted to satisfy blockchain's proof-of-work condition. This cryptographic structure ensures that if an attacker attempts to alter even a single transaction, they would need to recompute the hashes of all subsequent blocks in the chain, which is computationally infeasible. This feature makes blockchain a tamper-resistant and fraud-proof ledger, crucial for financial and management systems.

II. Smart Contracts for Automated Fraud Prevention

Smart contracts are self-executing programs stored on the blockchain that automatically enforce predefined rules and conditions without human intervention. These contracts eliminate the need for intermediaries, reducing processing time and operational costs while enhancing security. In fraud prevention, smart contracts validate transactions in real time, ensuring they meet security and compliance standards before approval. They can be programmed to automatically block suspicious activities, flag high-risk transactions, or initiate additional authentication steps for verification. By integrating AI models with smart contracts, businesses can develop intelligent fraud prevention mechanisms that react in real time, reducing false positives while maintaining a high level of security [20].

III. Transparent and Auditable Transactions:

One of the most powerful features of blockchain in fraud prevention is its ability to provide full transparency and auditability. Traditional databases require trusted third parties for auditing, which increases costs and potential security risks. Blockchain eliminates these inefficiencies by maintaining a public or permissioned ledger, where all transactions are timestamped, verifiable, and accessible for auditing. To further enhance security, blockchain employs a Merkle Tree structure, which organizes multiple transactions into a single, cryptographically secure hash [21]. This structure makes it computationally infeasible to alter past transactions without detection. The Merkle root is computed as:

$$M_R = hash(hash(T_1, T_2), hash\ (T_3, T_4))$$

Where T_1, T_2, T_3, T_4 are transaction hashes. Any modification in a transaction alters the Merkle root, ensuring fraud is detectable instantly.

By integrating blockchain with AI-driven fraud detection models, organizations can achieve a secure, transparent, and efficient fraud prevention framework that safeguards financial transactions while minimizing human intervention.

Conclusions

The fusion of Artificial Intelligence (AI) and Blockchain is revolutionizing fraud detection and anomaly prevention in modern management systems. Traditional fraud detection techniques, which rely on rule-based algorithms and manual auditing, struggle to keep pace with the evolving complexity of cyber threats and financial crimes. However, AI-powered models, such as tree-based classifiers, deep learning architectures (autoencoders, fully connected neural networks), and sequential models (LSTM, GRU), empower management systems to detect fraudulent patterns dynamically and in real time. These models enhance fraud detection accuracy while minimizing false positives, thereby improving decision-making and reducing financial risks. Statistical techniques, including the Five Number Summary, Z-Score Analysis, and Chi-Square Test, further refine anomaly detection by quantifying deviations in transaction behaviors. AI-driven fraud detection models leverage these statistical insights to identify outliers, recognize fraudulent trends, and adapt to emerging threats. Meanwhile, Blockchain technology enhances security, transparency, and integrity in fraud detection systems. With its decentralized, tamper-resistant ledger, blockchain eliminates single points of failure and prevents data manipulation. Smart contracts and cryptographic hashing ensure that transactions are immutable, verifiable, and auditable, making it difficult for fraudsters to exploit system vulnerabilities. The synergy between AI and Blockchain offers a comprehensive, intelligent, and secure management framework that enables businesses to proactively detect fraud, prevent financial losses, and enhance operational efficiency. As organizations increasingly adopt data-driven and decentralized management strategies, this integrated approach ensures a robust, transparent, and fraud-resilient ecosystem for the future.

References:

[1] Altuk, E. (2021). Detection and Prevention of Fraud in the Digital Era. , 126-137. https://doi.org/10.4018/978-1-7998-4805-9.CH009.

[2] Ashfaq, T., Khalid, R., Yahaya, A., Aslam, S., Azar, A., Alsafari, S., & Hameed, I. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. Sensors (Basel, Switzerland), 22. https://doi.org/10.3390/s22197162.

[3] Umer, K., & Kesavapattapa, R. (2024). INTEGRATING AI AND BLOCKCHAIN TECHNOLOGY FOR ROBUST FRAUD DETECTION MECHANISMS. International Journal of Research in Commerce and Management Studies. https://doi.org/10.38193/ijrcms.2024.6305.

[4] Yanamala, K. K. R. (2022). Dynamic bias mitigation for multimodal AI in recruitment ensuring fairness and equity in hiring practices. *Journal of Artificial Intelligence and Machine Learning in Management*, *6*(2), 51-61.

[5] Carta, S., Fenu, G., Recupero, D., & Saia, R. (2019). Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model. *J. Inf. Secur. Appl.*, 46, 13-22. https://doi.org/10.1016/J.JISA.2019.02.007.

[6] Udeh, E., Amajuoyi, P., Adeusi, K., & Scott, A. (2024). The role of big data in detecting and preventing financial fraud in digital transactions. *World Journal of Advanced Research and Reviews*. https://doi.org/10.30574/wjarr.2024.22.2.1575.

[7] Yanamala, K. K. R. (2023). AI and the future of cognitive decision-making in HR. *Applied Research in Artificial Intelligence and Cloud Computing*, *6*(9), 31-46.

[8] Xu, S., Lu, B., Baldea, M., Edgar, T., Wojsznis, W., Blevins, T., & Nixon, M. (2015). Data cleaning in the process industries. *Reviews in Chemical Engineering*, 31, 453 - 490. https://doi.org/10.1515/revce-2015-0022.

[9] Bahnsen, A., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Syst. Appl.*, 51, 134-142. https://doi.org/10.1016/j.eswa.2015.12.030.

[10] Starovoitov, V., & Golub, Y. (2021). Data normalization in machine learning. *Informatics*. https://doi.org/10.37661/1816-0301-2021-18-3-83-96.

[11] Li, A., Qiu, C., Smyth, P., Kloft, M., Mandt, S., & Rudolph, M. (2023). Deep Anomaly Detection under Labeling Budget Constraints. , 19882-19910. https://doi.org/10.48550/arXiv.2302.07832.

[12] Bao, Y., Ke, B., Li, B., Yu, Y., & Zhang, J. (2020). Detecting Accounting Fraud in Publicly Traded U.S. Firms Using a Machine Learning Approach. *Journal of Accounting Research*, 58, 199-235. https://doi.org/10.1111/1475-679x.12292.

[13] Yanamala, K. K. R. (2023). Transparency, privacy, and accountability in AI-enhanced HR processes. *Journal of Advanced Computing Systems*, *3*(3), 10-18.

[14] Warner, R. (2016). Using Z Scores for the Display and Analysis of Data. , 7-51. https://doi.org/10.1016/B978-0-12-804513-8.00002-X.

[15] Siegel, A. (2022). Chi-Squared Analysis. *Practical Business Statistics*. https://doi.org/10.1016/b978-0-12-385208-3.00017-1.

[16] Xu, B., Wang, Y., Liao, X., & Wang, K. (2023). Efficient Fraud Detection using Deep Boosting Decision Trees. *ArXiv*, abs/2302.05918. https://doi.org/10.48550/arXiv.2302.05918.

[17] Mienye, I., & Sun, Y. (2023). A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection. *IEEE Access*, 11, 30628-30638. https://doi.org/10.1109/ACCESS.2023.3262020.

[18] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Syst. Appl., 100, 234-245. https://doi.org/10.1016/j.eswa.2018.01.037.

[19] Noh, S. (2021). Analysis of Gradient Vanishing of RNNs and Performance Comparison. *Inf.*, 12, 442. https://doi.org/10.3390/info12110442.

[20] https://www.quantconnect.com/docs/v2/research-environment/applying-research/long-short-term-memory

[21] Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, 2, 1-10. https://doi.org/10.1186/S40854-016-0039-4.

[22] Raasetti, M. (2024). BLOCKCHAIN TECHNOLOGY'S ROLE IN SECURING DATA AND PREVENTING CYBERATTACKS: A DETAILED REVIEW. *ACADEMIC JOURNAL ON SCIENCE, TECHNOLOGY, ENGINEERING & MATHEMATICS EDUCATION*. https://doi.org/10.69593/ajsteme.v4i03.86.

[23] Louati, H., Louati, A., Almekhlafi, A., ElSaka, M., Alharbi, M., Kariri, E., & Altherwy, Y. (2024). Adopting Artificial Intelligence to Strengthen Legal Safeguards in Blockchain Smart Contracts: A Strategy to Mitigate Fraud and Enhance Digital Transaction Security. *Journal of Theoretical and Applied Electronic Commerce Research*. https://doi.org/10.3390/jtaer19030104.

[24] Mamulak, N., Miswadi, M., Julinaldi, J., Komarudin, R., & Syahputra, M. (2024). Blockchain Technology: Unlocking New Frontiers in Data Management and Transparency. *Global International Journal of Innovative Research*. https://doi.org/10.59613/global.v2i9.328.