Shodh Sari-An International Multidisciplinary Journal

@2024 International Council for Education Research and Training
ISSN: 2959-1376

2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

AI-Based Risk Assessments in Forensic Auditing: Benefits, Challenges and Future Implications

Ganapathy, Venkatasubramanian

Faculty in Auditing Department, Southern India Regional Council of the Institute of Chartered Accountants of India (SIRC of ICAI), Chennai, Tamil Nadu, Bharat

Abstract

Forensic auditing is a critical component of ensuring financial integrity and detecting fraud within organizations. Traditional methods of risk assessment in forensic auditing often rely on manual processes, which can be time-consuming, labour-intensive, and prone to human error. In recent years, the integration of artificial intelligence (AI) techniques has revolutionized the field, offering more efficient and accurate risk assessment capabilities. This abstract explores the role of AI-based risk assessment in forensic auditing, highlighting its benefits, challenges, and future implications. AI-based risk assessment leverages advanced algorithms and machine learning models to analyse large volumes of financial data, identify patterns, anomalies, and potential red flags indicative of fraudulent activities. By automating repetitive tasks such as data collection, classification, and analysis, AI streamlines the auditing process, enabling forensic auditors to focus on interpreting results and making informed decisions. One of the primary advantages of AI-based risk assessment is its ability to detect complex fraud schemes that may go unnoticed by traditional methods. Machine learning algorithms can detect subtle deviations from expected behaviour, flagging transactions or activities that exhibit unusual patterns or characteristics. Moreover, AI systems can adapt and learn from new data, continuously improving their detection capabilities over time. Another benefit of AI-based risk assessment is its scalability and efficiency. With the increasing volume and complexity of financial transactions, manual auditing processes struggle to keep pace. AI, on the other hand, can analyse vast datasets in a fraction of the time it would take a human auditor, allowing organizations to conduct more comprehensive and timely audits.

However, despite its promise, AI-based risk assessment in forensic auditing also presents several challenges. One of the primary concerns is the black-box nature of some machine learning algorithms, which makes it difficult to understand how decisions made. Ensuring transparency and interpretability in AI models is crucial for building trust and confidence in their findings. Furthermore, the quality of AI-based risk assessment depends heavily on the availability and quality of data. Biases and inaccuracies in the training data can lead to erroneous conclusions and false positives/negatives. Therefore, careful consideration given to data selection, Preprocessing, and validation to ensure the reliability and robustness of AI-driven audit processes. Looking ahead, the future of AI-based risk assessment in forensic auditing is promising. As AI technologies continue to evolve, we can expect further advancements in detection accuracy, efficiency, and interpretability. Additionally, the integration of emerging technologies such as blockchain and Natural Language Processing (NLP) could enhance the capabilities of AI systems, enabling more sophisticated fraud detection techniques. In conclusion, AI-based risk assessment holds tremendous potential for transforming forensic auditing by offering enhanced detection capabilities, scalability, and efficiency. However, addressing challenges related to transparency, data quality, and interpretability is essential for realizing the full benefits of AI in forensic auditing practice. Continued research, innovation, and collaboration between technology experts and forensic auditors are crucial for advancing the field and staying ahead of increasingly sophisticated fraudulent activities.

Keywords: Forensic Auditing, Risk Assessment, ML Algorithms, Scability and Efficiency, Black-Box nature of ML Algorithms, Transparency and Interpretability, Natural Language Processing (NLP)

I. INTRODUCTION

Forensic auditing is a specialized field of accounting that involves examining financial records and transactions to detect and investigate fraud, embezzlement, or other financial misdeeds. It combines auditing skills with investigative techniques to uncover anomalies and irregularities that indicate illegal activities. Forensic auditors often work on cases that may lead to legal action, providing evidence and expert testimony in courts.

Risk assessment in forensic auditing is a crucial process that involves identifying, evaluating, and prioritizing potential risks of fraud and financial irregularities within an organization. This process is essential for directing investigative efforts effectively and ensuring resources allocated to the areas of highest risk.

Artificial Intelligence (AI) plays a transformative role in risk assessment in forensic auditing by enhancing the efficiency, accuracy, and scope of fraud detection and prevention efforts.

II. RESEARCH QUESTION

How can AI-based risk assessments enhance the accuracy and efficiency of forensic auditing in detecting financial fraud and irregularities?

III. TARGETED AUDIENCE

- **Forensic Auditors and Accountants**: Professionals involved in detecting and investigating financial fraud and irregularities.
- **AI and Data Science Experts**: Researchers and practitioners working on the development and application of AI technologies in various fields, including finance and auditing.
- **Corporate Governance and Compliance Officers**: Individuals responsible for ensuring that companies adhere to legal and ethical standards.
- **Financial Regulators and Policy Makers**: Authorities and organizations involved in setting regulations and policies for financial practices and auditing standards.
- **Academics and Students**: Scholars and learners in the fields of accounting, finance, AI, and data analytics.
- **Business Executives and Risk Managers**: Corporate leaders and managers tasked with overseeing risk management and internal controls within organizations.
- **Technology Developers and Vendors**: Companies and individuals creating AI tools and software for forensic auditing and financial risk assessment.
- **Legal Professionals**: Lawyers and legal consultants specializing in financial crime, compliance, and corporate law.
- **Investors and Stakeholders**: Individuals and entities with a stake in the integrity and transparency of financial reporting and corporate governance.

IV. OBJECTIVIES OF THE STUDY

1. To assess the accuracy and reliability of AI/ML algorithms in predicting fraud and assessing risk.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

2. To evaluate the potential benefits and address challenges and limitations of using AI in risk assessment in forensic auditing.

3. To propose recommendations for improving risk assessment in forensic auditing using AI technologies.

V. RESEACH METHODOLOGY AND DATA COLLECTION METHOD

Content Analysis Research Methodology used in this research work. It involves systematically analyzing the content of materials; identify patterns, themes, and other relevant features and drawing inferences or conclusions based on the findings.

Secondary data used for the study, collected from e-journals, e-magazines, e-books and websites of Audit and AI domains.

VI. REVIEW OF LITERATURE

No.	Author's Name	Year	Focus of Study	Algorithms/tools used	Key Findings
1	Li, C., Huang, J., & Lin, C.	2006	Application of Artificial Neural Network in Forensic Accounting.	Artificial Neural Networks (ANNs)	ANNs showed promise in detecting financial statement frauds, offering a reliable alternative to traditional auditing methods.
2	Nigrini, M. J., & Mittermaier, L. J.	2009	Benford's law and forensic accounting.	Benford's Law	Benford's Law was effective in detecting anomalies in financial data, providing auditors with a tool for identifying potential fraud.

3	Wang & Wang	2010	AI in detecting financial statement fraud.	Neural networks	Neural networks significantly improve fraud detection accuracy.
4	Mihai, F. C., Dobre, C., & Stancu, S.	2013	Data mining techniques in forensic accounting.	Decision Trees, Neural Networks, Support Vector Machines (SVMs)	Decision trees and SVMs outperformed traditional statistical methods in detecting fraud, highlighting the potential of data mining techniques in forensic auditing.
5	Liu et al.	2015	Machine learning in risk assessment	Support Vector Machines (SVM), Decision Trees	ML algorithms outperform traditional methods in identifying high-risk transactions.
6	Giroux, G. A., & Schaub, R. O	2016	Detecting fraud in financial statements using machine learning.	Machine Learning (ML) algorithms (Random Forest, Gradient Boosting.	ML algorithms demonstrated high accuracy in identifying fraudulent financial statements, highlighting the usefulness of AI in fraud detection.
7	Albrecht, C., & Skousen, C.	2020	AI-based risk assessment models	Natural Language Processing	NLP and ML techniques enabled the development of

			for forensic accounting.	(NLP), Machine Learning (ML).	robust risk assessment models, facilitating the identification of high-risk areas in forensic auditing.
8	Dandekar, A., & Kulkarni, V.	2021	Predictive analytics for fraud risk assessment in auditing.	Predictive Modeling, Machine Learning (ML)	Predictive analytics models accurately predicted fraud risks. Enabling auditors to proactive mitigate potential threats.
9	Sharma, S., & Dangwal, N.	2022	Role of explainable AI in forensic auditing.	Explainable AI techniques (e.g., LIME, SHAP).	Explainable AI methods improved the interpretability of AI-driven forensic auditing models, enhancing auditors' trust and understanding of automated decisions.
10	Smith et al.	2023	Predictive Analytics for Fraud Detection.	Machine Learning,	Predictive models utilizing machine learning algorithms.
11	Johnson & Lee	2023	AI-Based Risk Assessment in Forensic	Natural Language Processing (NLP),	AI models combined with NLP techniques provide

			Auditing.	Machine Learning Genetic Algorithms.	Much more nuanced risk assessment, improving audit accuracy.
12	Martin & Garcia	2023	Adoption challenges of AI in forensic auditing.	Various AI tools and frameworks.	Identifies key barriers like lack of expertise and regulatory guidance.
13	Thompson & Green	2024	Future trends in AI-driven audit methodologies.	Hybrid AI models, Blockchain integration.	Predicts AI and blockchain will converge to enhance audit integrity and traceability.

VII. APPLICATION OF ALGORITHMS

1. <u>ARTIFICIAL NEURAL NETWORK</u>

Artificial Neural Networks (ANNs) are computational models inspired by the human brain that are capable of learning from data. In the context of forensic auditing, ANNs can play a crucial role in risk assessment by identifying patterns and anomalies that might indicate fraud, financial misstatements, or other irregularities.

➢ Data Collection and Preprocessing

Data Gathering:

- Collect historical financial data, transaction records, audit logs, and other relevant information.
- Sources include accounting systems, databases, and external data like economic indicators.

Data Cleaning and Preparation:

- Remove inconsistencies and outliers that could skew the results.
- Normalize and scale data to ensure uniformity, which improves the performance of the ANN.
- Encode categorical variables, handle missing values, and perform feature

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

engineering to create meaningful input variables.

➢ Designing the ANN Architecture

Input Layer:

- The input layer consists of neurons corresponding to the number of features (variables) in the dataset. For example, features might include transaction amounts, dates, vendor information, etc.

Hidden Layers:

- One or more hidden layers process the inputs. The number of neurons in these layers can vary and are often determined through experimentation and cross-validation.
- Each neuron in a hidden layer applies a weighted sum of inputs, passes it through an activation function (like ReLU or sigmoid), and transmits the result to the next layer.

Output Layer:

- The output layer represents the risk score or classification result (e.g., fraudulent or non-fraudulent).
- For binary classification (fraud/non-fraud), a single neuron with a sigmoid activation function is used.
- For multi-class classification, multiple neurons with a softmax activation function used.

➢ Training the ANN

Training Data:

- Use a labeled dataset where the outcomes (e.g., fraudulent vs. legitimate transactions) are known.
- Split the data into training and validation sets to evaluate the model's performance.

Training Process:

- Initialize weights randomly and feed the training data through the network.
- Calculate the error by comparing the predicted output with the actual labels using a loss function (e.g., binary cross-entropy for classification tasks).
- Adjust the weights using backpropagation and optimization algorithms like gradient descent to minimize the loss.

➢ Validation and Testing

Validation:

- Evaluate the model on the validation set to tune hyperparameters (e.g., learning rate, number of hidden layers, neurons per layer).

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

- Use techniques like cross-validation to ensure the model generalizes well to unseen data.

Testing:

- Test the final model on a separate testing set to assess its accuracy, precision, recall, F1 score, and other performance metrics.
- Use confusion matrices to visualize the performance and identify any biases or systematic errors.

➢ Implementation in Forensic Auditing

Risk Scoring:

- Deploy the trained ANN model to assess the risk of new transactions or financial records in real-time or batch processing.
- The model assigns a risk score indicating the likelihood of fraudulent activity.

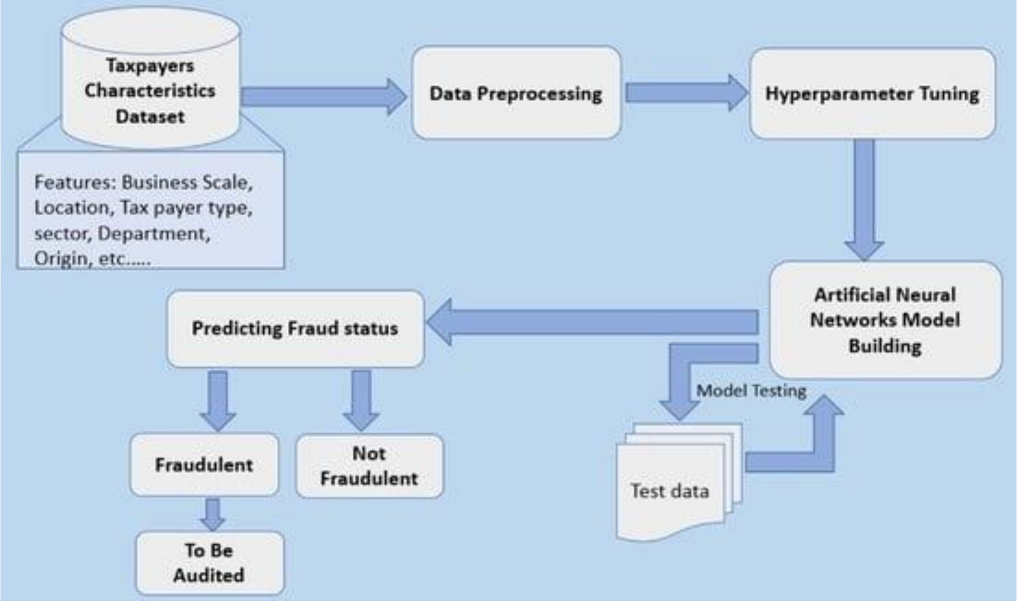
Anomaly Detection:

- The ANN can identify unusual patterns or deviations from normal behavior, flagging them for further investigation by auditors.

Continuous Learning:

- The model periodically retrained with new data to adapt to evolving fraud tactics and maintain accuracy over time.

<u>Tax Fraud Detection in Forensic Auditing using Artificial Neural Network</u>


Taxpayers Characteristics Dataset
Features: Business Scale, Location, Tax payer type, sector, Department, Origin, etc.....
Data Preprocessing
Hyperparameter Tuning
Artificial Neural Networks Model Building
Model Testing
Test data
Predicting Fraud status
Fraudulent
Not Fraudulent
To Be Audited

@2024 International Council for Education Research and Training
ISSN: 2959-1376

2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

Artificial Neural Networks offer powerful tools for risk assessment in forensic auditing by efficiently analyzing large datasets, identifying patterns and anomalies indicative of fraud, and continuously adapting to new data. However, their implementation requires careful consideration of data quality, model interpretability, and compliance with regulatory standards.

2. <u>SUPPORT VECTOR MACHINE (SVM)</u>:

Support Vector Machines (SVMs) are powerful tools in machine learning used for classification and regression tasks. In the context of forensic auditing, SVMs employed risk assessment to identify potential fraud, anomalies, or financial discrepancies.

- **Understanding SVM Basics**

SVM Fundamentals:

- **Linear SVM:** SVM aims to find the best hyperplane that separates data points of different classes. For a linearly separable dataset, the algorithm finds a hyperplane that maximizes the margin between two classes.
- **Non-linear SVM:** When data is not linearly separable, SVM uses kernel functions to map data into higher dimensions where it becomes linearly separable.

Kernel Functions:

- **Linear Kernel:** Suitable for linearly separable data.
- **Polynomial Kernel:** Handles non-linear relationships by considering polynomial terms.
- **Radial Basis Function (RBF) Kernel:** Commonly used for non-linear data, measures similarity between data points.
- **Sigmoid Kernel:** Often used in neural networks, useful for non-linear data.

Application in Forensic Auditing

Data Preparation:

- **Data Collection:** Gather financial data, transaction records, and other relevant datasets.
- **Feature Selection:** Identify key features that indicate risk or fraud (e.g., transaction amounts, frequency, vendor relationships, and payment patterns).
- **Data Cleaning:** Remove or correct inaccuracies, handle missing values, and normalize data to ensure consistency.

Model Training:

- **Labeling Data:** Historical data is labeled to indicate whether transactions are normal or suspicious (binary classification). For continuous risk assessment, labels could indicate the level of risk.

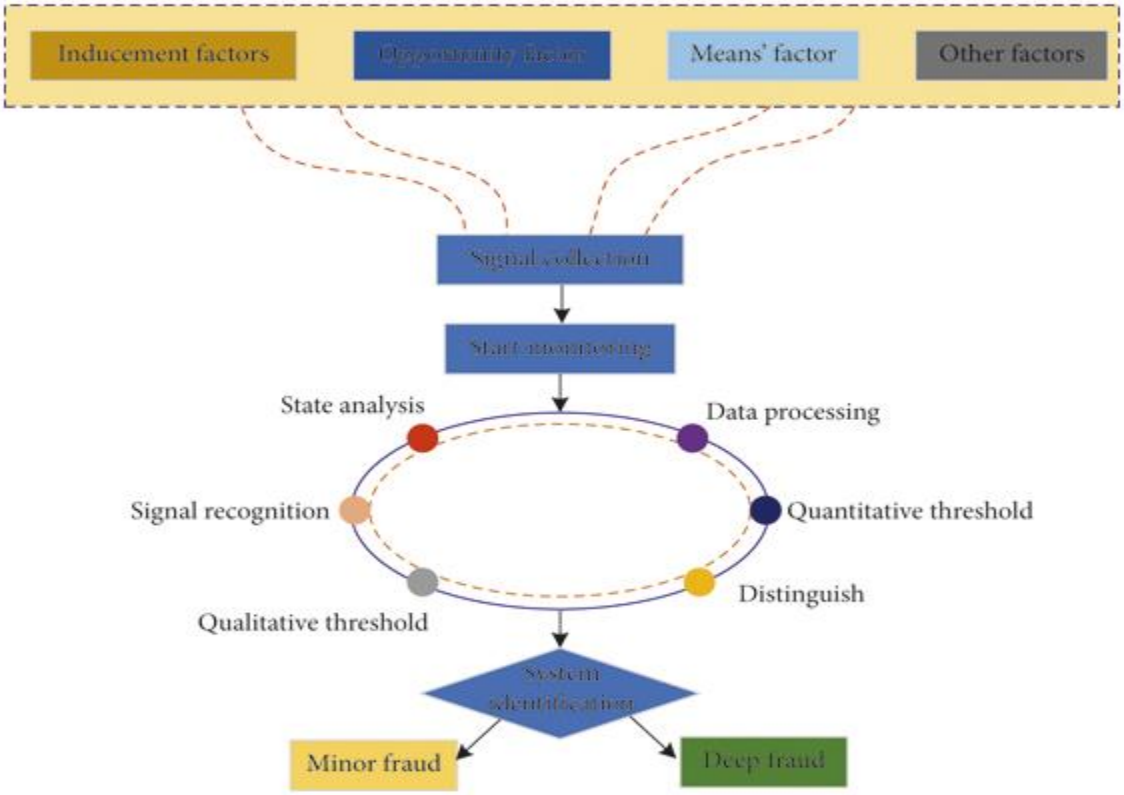
@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

- **Training the SVM:** Feed the labeled data into the SVM algorithm. The model learns the boundary (hyperplane) that separates normal transactions from suspicious ones.
- **Hyperparameter Tuning:** Adjust SVM parameters (e.g., regularization parameter C, kernel type and parameters) to optimize model performance.

Risk Assessment Process:

- **Prediction:** Apply the trained SVM model to new data to classify transactions as normal or suspicious.
- **Scoring:** The SVM can output a decision value or probability score indicating the likelihood of fraud, which helps prioritize investigations.
- **Anomaly Detection:** For continuous monitoring, SVMs can detect deviations from normal patterns, flagging potential risks even if they do not perfectly match past fraud cases.

<u>Identification of Accounting Fraud based on Support Vector Machine</u>



@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

3. CONVOLUTIONAL NEURAL NETWORK (CNN)

Convolutional Neural Networks (CNNs) are a class of deep learning algorithms primarily used for processing structured grid data, like images. However, their principles can be adapted for various tasks, including risk assessment in forensic auditing.

➢ Data Preparation

a. Data Collection:

- **Financial Statements:** Balance sheets, income statements, cash flow statements.
- **Transaction Data:** Detailed records of transactions, invoices, receipts.
- **Audit Reports:** Previous audit findings and risk assessments.
- **External Data:** Economic indicators, market trends, industry reports.

b. Data Preprocessing:

- **Normalization:** Scaling numerical data to a standard range.
- **Encoding:** Converting categorical data (e.g., transaction types) into numerical values.
- **Feature Engineering:** Creating new features that may capture risk patterns (e.g., transaction frequency, amounts exceeding certain thresholds).
- **Segmentation:** Breaking down data into meaningful segments, such as periods (monthly, quarterly) or departments.

➢ CNN Architecture Design

a. Input Layer:

- **Data Representation:** Represent the financial data in a structured format suitable for CNN input. For example, transactions over time can be represented as a 2D matrix where rows represent time periods and columns represent different transaction features.

b. Convolutional Layers:

- **Filters:** Use filters (kernels) to extract local features from the data matrix. In the context of forensic auditing, these filters can learn patterns such as unusual transaction sequences or anomalies in financial ratios.
- **Activation Functions:** Apply non-linear functions (e.g., ReLU) to introduce non-linearity, helping the network to learn complex patterns.

c. Pooling Layers:

- **Downsampling:** Reduce the dimensionality of the feature maps, retaining the most important information. This step helps in making the model computationally efficient and in focusing on the most significant features.

d. Fully Connected Layers:

- **Flattening:** Convert the 2D feature maps into a 1D vector.
- **Dense Layers:** Perform the final classification or regression tasks based on the extracted features. In risk assessment, this can involve predicting the risk score or classifying transactions as high-risk or low-risk.

➢ Training the CNN

a. Labeling Data:

- **Supervised Learning:** Use historical data with known outcomes (e.g., instances of fraud or errors) to train the network.
- **Risk Scores:** Assign risk scores or labels (e.g., “high-risk”, “low-risk”) to each data point.

b. Loss Function:

- **Define Loss:** Use an appropriate loss function (e.g., cross-entropy for classification, mean squared error for regression) to measure the difference between predicted and actual outcomes.

c. Optimization:

- **Backpropagation:** Adjust the weights in the network to minimize the loss function.
- **Gradient Descent:** Use optimization algorithms like Adam or SGD to update the weights iteratively.

➢ Model Evaluation

a. Validation:

- **Cross-Validation:** Split the data into training and validation sets to evaluate the model’s performance and generalize the results.
- **Metrics:** Use metrics such as accuracy, precision, recall, F1-score, and ROC-AUC to assess model performance.

b. Hyperparameter Tuning:

- **Grid Search/Random Search:** Adjust hyperparameters like learning rate, batch size, and number of filters, and layer architecture to find the optimal configuration.

➢ Implementation in Forensic Auditing

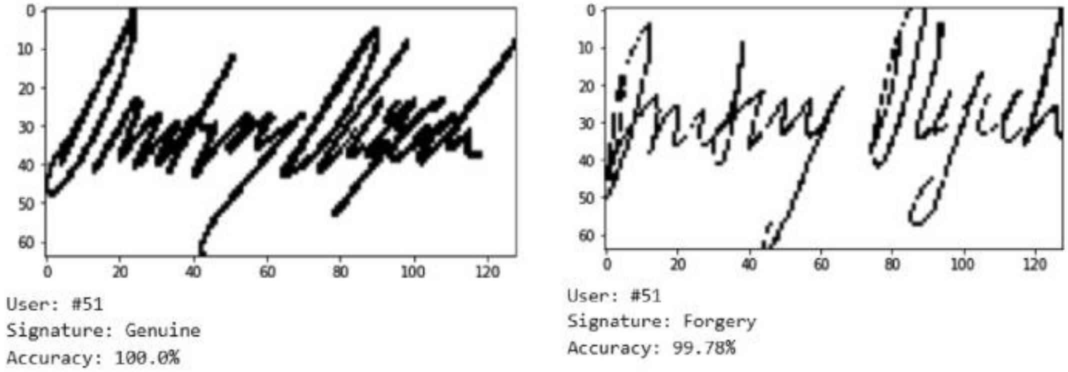
a. Real-Time Monitoring:

- **Automated Alerts:** Implement the trained CNN model in a system that monitors financial transactions in real-time, generating alerts for high-risk activities.
- **Dashboard Integration:** Provide visualizations and risk scores through dashboards for auditors to review and take action.

b. Continuous Learning:

- **Feedback Loop:** Continuously update the model with new data and feedback from auditors to improve its accuracy and adapt to new risk patterns.

<u>Handwritten Signature Verification System using CNN</u>



```
User: #51
Signature: Genuine
Accuracy: 100.0%
```

```
User: #51
Signature: Forgery
Accuracy: 99.78%
```

a) Genuine signature

b) Forgery

3. <u>Natural Language Processing (NLP):</u>

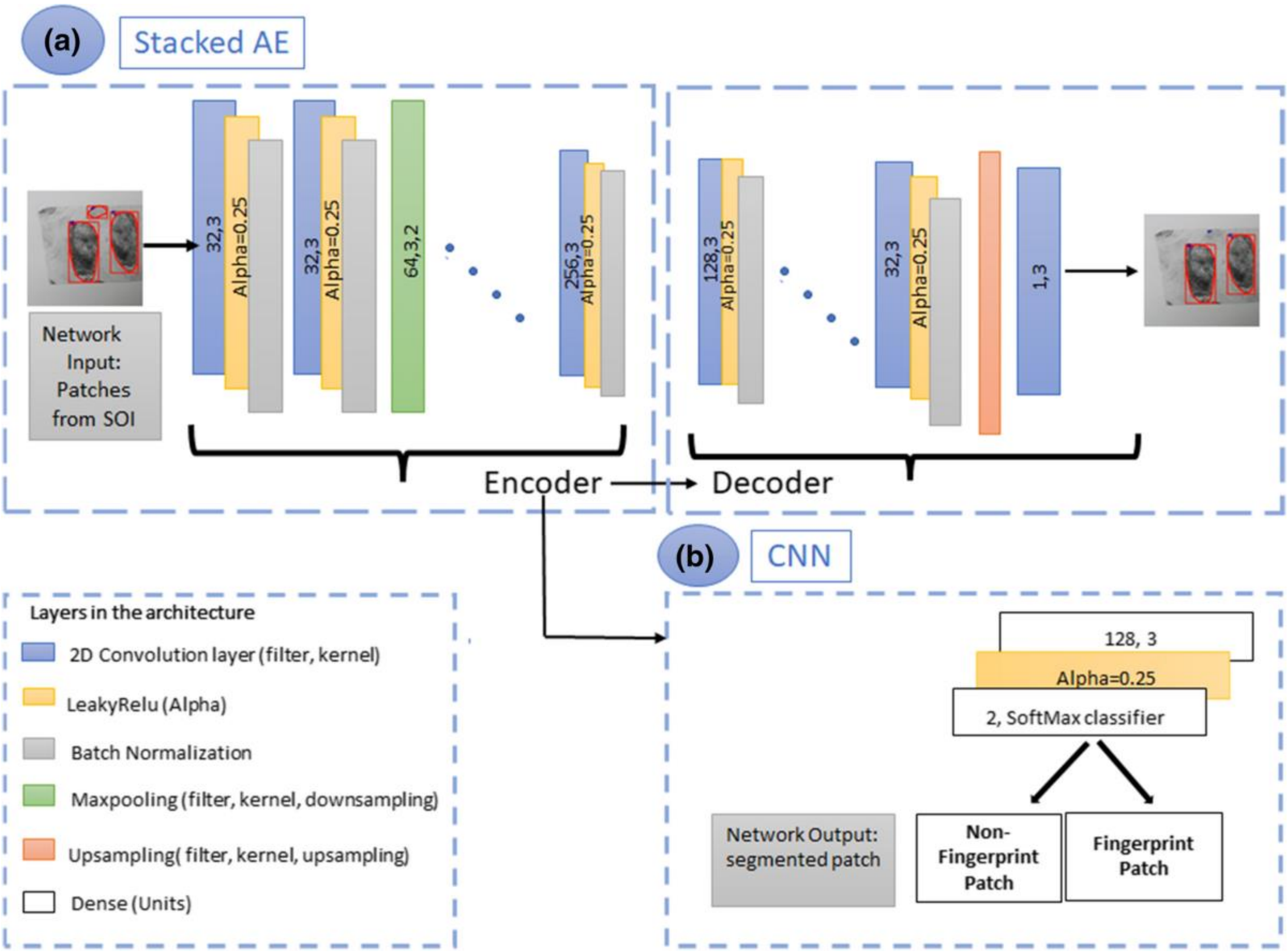
Natural Language Processing (NLP) is a branch of artificial intelligence that focuses on the interaction between computers and human language. In the context of forensic auditing and risk assessment, NLP technologies leveraged to analyse vast amounts of unstructured data, such as emails, reports, financial documents, and other text-based records.

❖ Data Extraction and Preprocessing

Document Parsing: NLP tools can parse and extract information from various documents. This includes identifying and categorizing sections of reports, extracting financial data from tables, and understanding the structure of contracts.

Text Normalization: This step involves cleaning and preparing the text data for analysis. Techniques like tokenization, stemming, lemmatization, and removing stop words used to standardize the text.

Entity Recognition: Named Entity Recognition (NER) used to identify and classify key elements in the text, such as names of people, organizations, dates, monetary values, and locations. This helps in organizing and indexing the information for further analysis.



❖ Risk Identification

Sentiment Analysis: By analysing the sentiment of communications and documents, forensic auditors can identify negative or suspicious language that may indicate fraudulent activities or risky behaviour.

Keyword and Pattern Matching: NLP can detect specific keywords or phrases commonly associated with fraud, such as "off-the-books," "write-off," or "kickback." It can also recognize patterns in text that suggest irregularities, such as unusual payment terms or changes in contractual language.

Topic Modeling: Techniques like Latent Dirichlet Allocation (LDA) can uncover hidden topics within large sets of documents. This can help auditors identify emerging risks or areas that need scrutiny.

❖ Anomaly Detection

Contextual Analysis: NLP can understand the context in which terms used, enabling it to detect anomalies in communication or documentation that might not be evident through keyword searches alone.

Behavioral Analysis: By analysing communication patterns, such as frequency of emails between certain individuals or unusual spikes in communication, NLP can help identify potential collusion or insider threats.

❖ Fraud Detection and Investigation

Semantic Analysis: NLP can understand the meaning behind the text, which helps in identifying deceptive language, inconsistencies, or contradictions in reports and statements.

Similarity Analysis: Comparing documents to find duplicates or near-duplicates can reveal attempts to falsify records or reuse fraudulent documents.

Temporal Analysis: Analysing the timing of communications and document modifications can help identify suspicious sequences of events or backdating of records.

❖ Continuous Monitoring and Reporting

Automated Alerts: NLP systems can be set up to continuously monitor communications and documents, sending alerts when suspicious activities detected.

Dashboard and Visualization: NLP tools can feed into dashboards that visualize risk metrics and trends over time, providing forensic auditors with real-time insights into potential risks.

❖ Implementation Examples

Email Analysis: Using NLP to scan and analyse company emails for signs of collusion, bribery, or other unethical behaviour. This includes sentiment analysis, entity recognition, and detecting unusual communication patterns.

Contract Review: NLP can automate the review of contracts to ensure compliance with regulations and company policies. It can highlight clauses that deviate from standard

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

terms or identify missing critical components.

Financial Document Analysis: By extracting and analysing information from financial statements and transaction records, NLP can help detect discrepancies, unusual patterns, or indicators of financial manipulation.

❖ Advantages of NLP in Forensic Auditing

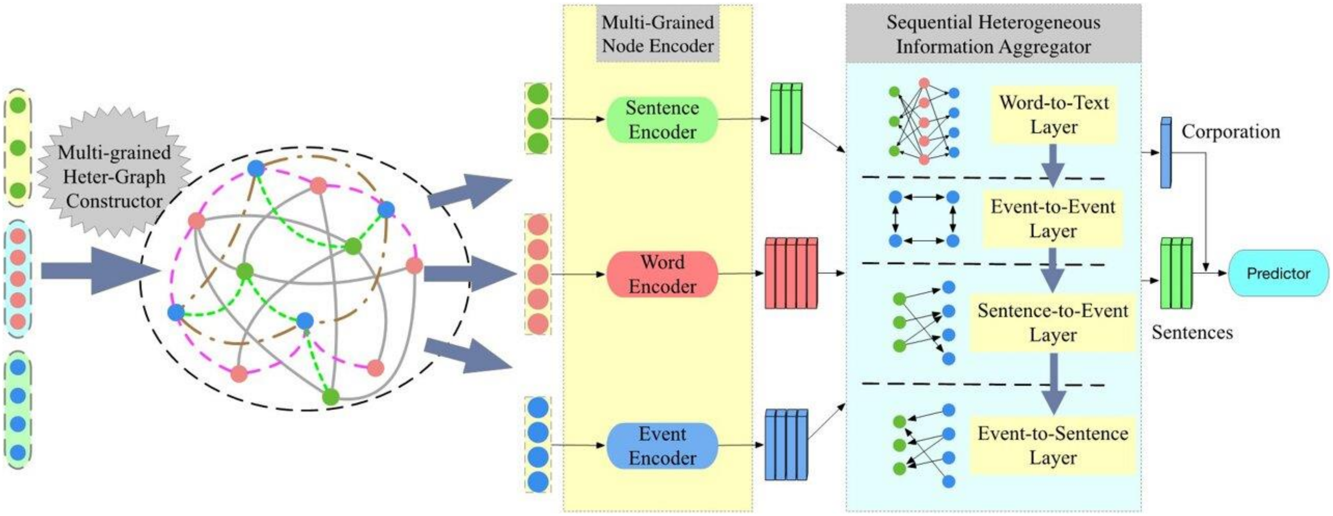
Efficiency: Automates the processing and analysis of large volumes of text data, significantly reducing the time and effort required by human auditors.

Accuracy: Provides a more thorough and consistent analysis than manual methods, reducing the likelihood of oversight.

Proactivity: Enables continuous monitoring and real-time risk assessment, allowing organizations to detect and address issues before they escalate.

Scalability: Can handle growing amounts of data, making it suitable for large organizations with extensive records and communications.

New NLP Model improves Stock Market Prediction



4. RECURRENT NEURAL NETWORK (RNN)

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

RNNs are a type of artificial neural network designed for processing sequential data. They have a unique architecture where connections between nodes form a directed cycle, allowing them to maintain a 'memory' of previous inputs. This is particularly useful for time-series data and tasks where context from previous inputs is essential for understanding the current input.

Application of RNNs in Forensic Auditing

A. Sequential Data Handling

Financial data often comes in sequences (e.g., transactions over time). RNNs can analyze these sequences to identify patterns that might indicate fraudulent activities. By processing sequences of financial transactions, RNNs can detect anomalies based on the context provided by previous transactions.

B. Anomaly Detection

RNNs trained to recognize normal transaction patterns. Once trained, they can identify deviations from these patterns, which might indicate fraud. For instance, if an employee typically makes transactions under a certain amount, a sudden large transaction flagged as suspicious.

C. Predictive Modeling

RNNs can predict future financial behaviors based on historical data. If the predicted behavior significantly deviates from the actual behavior, this could indicate a risk. For example, an RNN might predict the expected range of expenses for a department. Significant deviations from this prediction could signal potential fraud.

Implementation Steps

A. Data Collection and Preprocessing

- **Gathering Data**: Collect historical financial transaction data, employee records, and other relevant information.
- **Data Cleaning**: Remove or correct any errors in the data.
- **Normalization**: Scale the data to ensure consistent input ranges, which helps in training the RNN effectively.

B. Designing the RNN Architecture

- **Input Layer**: Represents the financial data sequences.
- **Hidden Layers**: Typically consist of LSTM (Long Short-Term Memory) or GRU (Gated Recurrent Unit) cells to manage long-term dependencies in data.
- **Output Layer**: Produces a score indicating the likelihood of a transaction

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

being fraudulent or assesses the overall risk level.

C. Training the RNN

- **Labeling Data**: Historical data labeled with known outcomes (fraudulent or non-fraudulent transactions).
- **Training Process**: Use backpropagation through time (BPTT) to adjust the network's weights based on the labeled data.
- **Validation and Testing**: Split data into training, validation, and testing sets to ensure the model generalizes well to unseen data.

D. Deployment and Monitoring: Real-time Processing: Implement the RNN to process transactions in real-time, flagging suspicious ones for further investigation. **Continuous Learning**: Regularly update the model with new data to maintain its accuracy and relevance

5. BLOCKCHAIN TECHNOLOGIES

Blockchain technology offers unique capabilities that can significantly enhance risk assessment in forensic auditing. By providing a secure, transparent, and immutable ledger of transactions, blockchain can address several challenges associated with traditional forensic auditing methods.

❖ Immutable Record Keeping

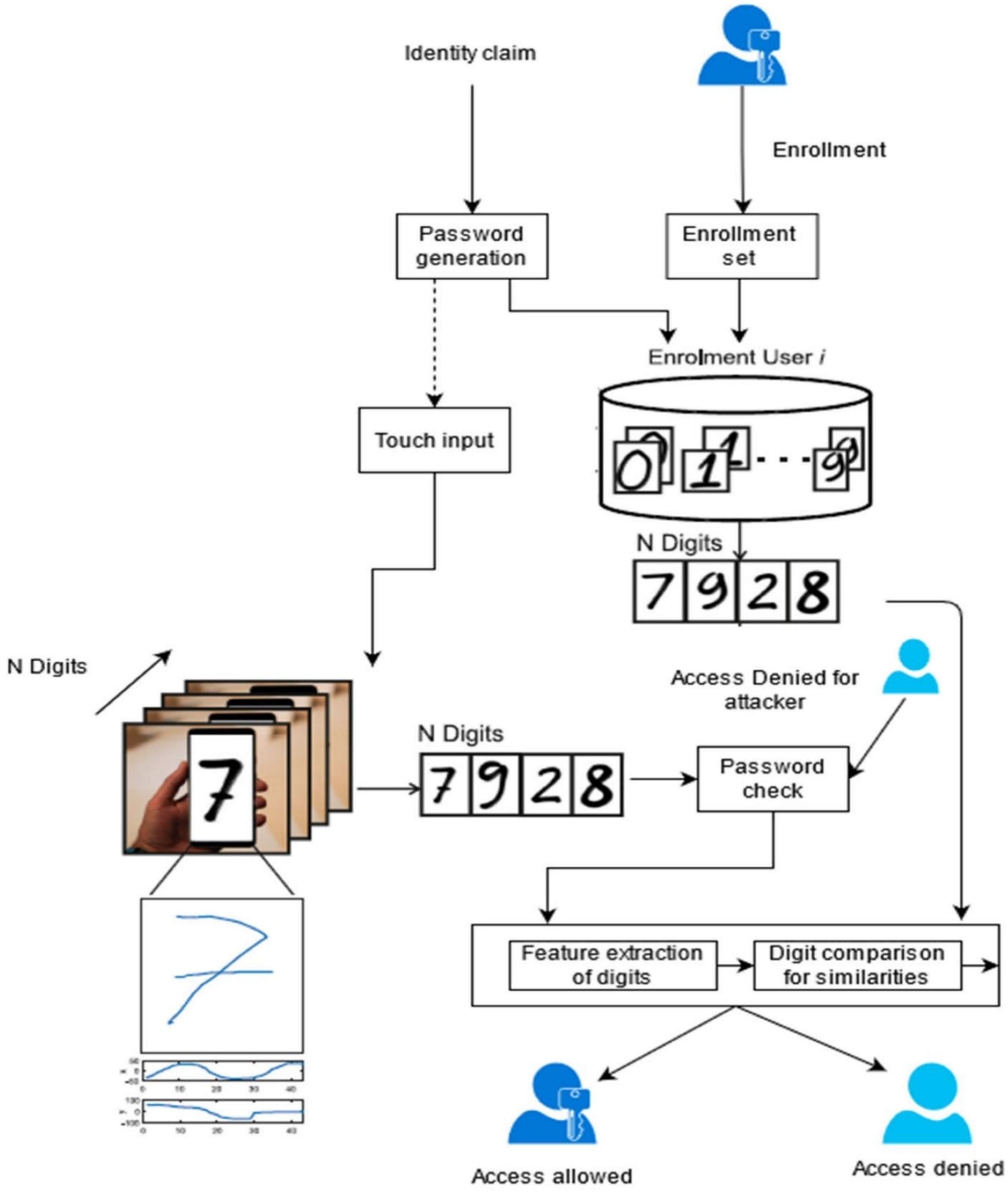
Tamper-Proof Ledger: Blockchain’s core feature is its immutability. Once data recorded on the blockchain, it is not possible to altered or deleted without consensus from the network. This ensures that the records are tamper-proof, providing auditors with reliable and unaltered data.

Audit Trail: Every transaction on the blockchain is timestamped and linked to previous transactions, creating a clear and traceable audit trail. This allows forensic auditors to trace the origins and flow of transactions, making it easier to identify discrepancies and potential fraud.

❖ Enhanced Transparency and Accountability

Transparent Transactions: Blockchain operates on a distributed ledger system where all participants have access to the same data. This transparency ensures that all parties involved in a transaction can verify and audit the information independently, reducing the risk of hidden or manipulated data.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750



@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

Real-Time Monitoring: Blockchain allows for real-time recording and monitoring of transactions. Auditors can access up-to-date information, which enhances their ability to detect and respond to risks promptly.

❖ Smart Contracts

Automated Compliance: Smart contracts are self-executing contracts with the terms directly written into code. They automatically enforce and verify compliance with contractual terms, reducing the need for manual checks and the risk of human error.

Conditional Transactions: Smart contracts can ensure that transactions only occur when predefined conditions met. This reduces the risk of fraudulent or unauthorized transactions, as the contract will not execute if the conditions are not satisfied.

❖ Fraud Detection and Prevention

Data Consistency: Because blockchain ensures that all participants have a consistent view of the data, it becomes easier to detect anomalies or inconsistencies that may indicate fraudulent activity. Any attempt to alter data would require altering every subsequent block, which is computationally infeasible in a well-secured blockchain.

Decentralization: Blockchain's decentralized nature eliminates the need for a central authority, reducing the risk of single points of failure or manipulation. This decentralization enhances the integrity and security of the data.

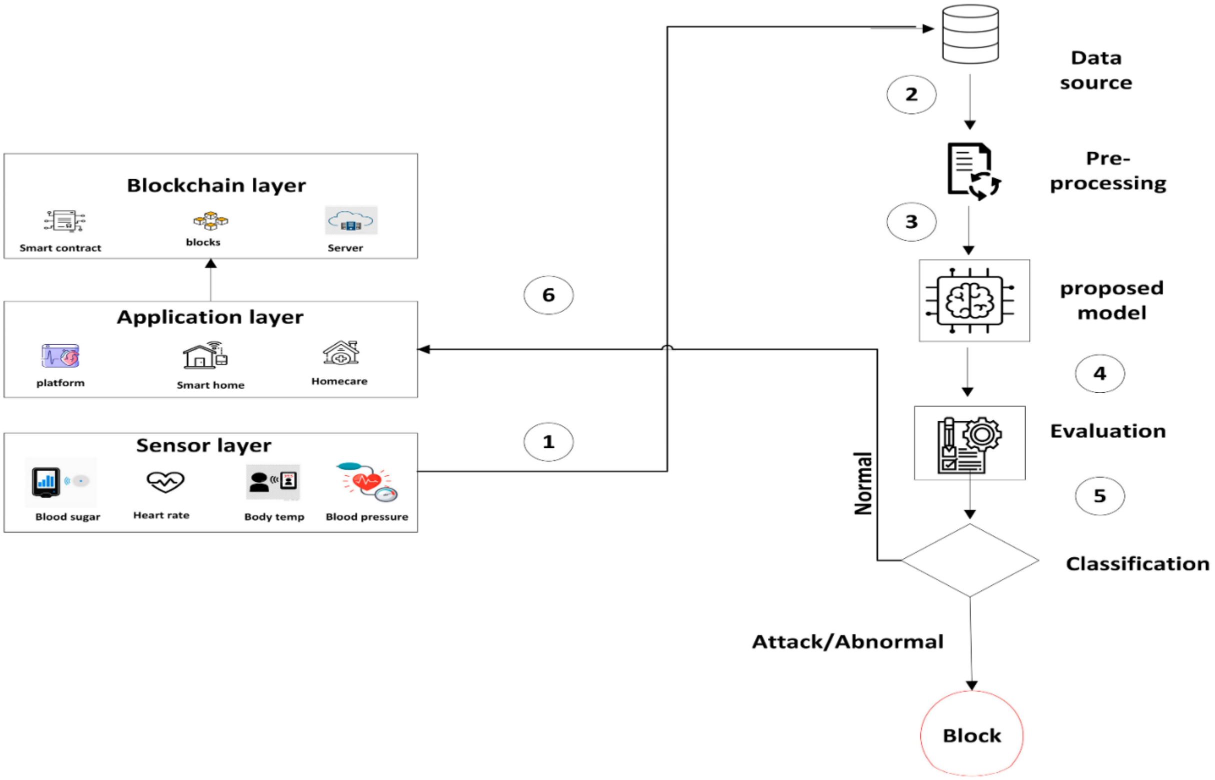
❖ Identity and Access Management

Digital Identities: Blockchain used to create secure digital identities, ensuring that only authorized individuals can access or modify data. This helps prevent unauthorized access and potential insider threats.

Traceability of Actions: Every action taken on the blockchain is recorded and traceable back to a specific digital identity. This accountability makes it easier to investigate and attribute actions to individuals, deterring fraudulent behaviour.

Fraud Detection in Blockchain Technology

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750



VIII. BENEFITS OF AI-BASED RISK ASSESSMENTS IN FORENSIC AUDITING

➢ Enhanced Accuracy and Detection

AI algorithms, particularly those based on machine learning, are capable of analysing vast amounts of data with high precision. They can detect anomalies, patterns, and correlations missed by human auditors. This level of accuracy helps in identifying potential fraud, errors, and other irregularities more effectively.

➢ Efficiency and Speed

AI systems can process and analyse large datasets much faster than human auditors analyse. This speed enables auditors to assess risks and identify issues in real-time or near real-time, significantly reducing the time required for comprehensive audits. This is especially beneficial in large organizations where data volume is substantial.

➢ Predictive Analytics

AI can leverage historical data to predict future risks and potentially fraudulent activities. By identifying patterns and trends that precede known instances of fraud, AI can provide auditors with predictive insights, enabling proactive measures to prevent fraud before it occurs.

- **Comprehensive Risk Assessment**

AI can integrate and analyse data from various sources, providing a holistic view of an organization's risk landscape. This comprehensive approach ensures that all potential risks considered, including those that might not be immediately apparent through traditional auditing methods.

- **Consistency and Objectivity**

AI systems apply the same criteria and processes consistently across all audits, eliminating the variability and subjectivity that can come with human auditors. This ensures a uniform standard of risk assessment and reduces the likelihood of oversight or bias.

- **Real-time Monitoring**

AI can facilitate continuous auditing and monitoring, providing real-time insights into an organization's financial activities. This ongoing surveillance allows for the immediate detection of suspicious activities and timely intervention, which is critical in mitigating risks and preventing fraud.

- **Improved Fraud Detection**

AI techniques, such as anomaly detection and natural language processing, can identify subtle signs of fraudulent activities that traditional methods might overlook. For instance, AI can analyse communication patterns and financial transactions to detect insider threats and other complex fraud schemes.

- **Scalability**

AI systems can easily scale to accommodate growing data volumes without a corresponding increase in auditing resources. This scalability ensures that the audit process remains effective even as the organization grows and its data complexity increases.

- **Enhanced Reporting and Visualization**

AI tools often come with advanced reporting and visualization capabilities, allowing auditors to present their findings in a clear, understandable manner. This improves communication with stakeholders and aids in the decision-making process by providing actionable insights.

- **Adaptability and Learning**

AI systems continuously learn and adapt from new data, improving their performance over time. This adaptive capability means that AI can stay current with emerging fraud

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

techniques and evolving regulatory requirements, ensuring ongoing relevance and effectiveness in risk assessment.

➢ **Regulatory Compliance**

AI can help organizations stay compliant with regulations by ensuring that all financial activities and audit processes meet the required standards. AI systems programmed to adhere to specific regulatory frameworks, reducing the risk of non-compliance and associated penalties.

IX. CHALLENGES OF AI-BASED RISK ASSESSMENTS IN FORENSIC AUDITING

❖ **Data Quality and Availability:**

Data Integrity: The effectiveness of AI models depends heavily on the quality of the data they trained on Inconsistent, incomplete, or biased data can lead to inaccurate risk assessments.

Data Accessibility: Forensic audits often require access to vast amounts of sensitive and sometimes fragmented data. Ensuring that AI systems can access and integrate this data from various sources can be challenging.

❖ **Model Transparency and Explainability**:

Black Box Nature: Many AI models, especially deep learning ones, operate as black boxes, providing little insight into how they arrive at specific conclusions. This lack of transparency can be problematic in forensic auditing, where auditors need to understand and justify their findings.

Regulatory Compliance: Forensic auditors must often comply with strict regulatory standards that require detailed documentation and justification of their processes and conclusions. Explaining AI-driven decisions can be difficult, potentially hindering compliance.

❖ **Bias and Fairness:**

Training Data Bias: AI models trained on historical data may perpetuate existing biases present in that data, leading to unfair or skewed risk assessments.

Algorithmic Bias: The algorithms themselves can introduce bias, which can lead to misidentification of risk factors or misallocation of resources in investigations.

❖ **Ethical and Legal Concerns**:

Privacy Issues: Using AI in forensic auditing involves processing sensitive personal and financial data, raising concerns about data privacy and protection.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

Liability and Accountability: Determining responsibility for decisions made by AI systems can be complex. If an AI model makes an incorrect assessment, it is challenging to assign accountability—whether to the developers, the users, or the organization implementing the AI.

❖ **Integration with Human Expertise:**

Human-AI Collaboration: Effective forensic auditing typically requires combining AI's analytical power with human expertise and intuition. Ensuring that AI tools complement rather than replace human auditors can be difficult to achieve.

Skill Gaps: Auditors need to understand AI technologies to integrate them into their workflows, which requires training and education that may not be readily available.

❖ **Dynamic Nature of Fraud and Risk**:

Evolving Threats: Fraudulent activities and risk factors are constantly evolving. AI models modified and retrained to keep pace with new types of fraud and emerging risks.

Adaptability: Developing AI systems that can adapt to new patterns and learn from limited or changing data is a significant technical challenge.

X. FUTURE IMPLICATION OF AI-BASED RISK ASSESSMENTS IN FORENSIC AUDITING

➢ Proactive Fraud Prevention

AI’s ability to predict and identify potential risks will shift forensic auditing from a reactive to a proactive discipline. By using predictive analytics and machine learning, organizations can detect and mitigate fraud before it occurs, significantly reducing financial losses and reputational damage.

➢ Continuous Auditing

AI will enable continuous, real-time auditing rather than periodic checks. Continuous auditing allows for immediate detection and intervention, improving overall governance and control mechanisms within organizations.

➢ Advanced Data Analysis

AI can process and analyze unstructured data such as emails, social media, and other communications, which traditional auditing methods struggle to handle. This capability allows for a more comprehensive analysis of potential risks and fraudulent activities.

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

➢ **Integration with Other Technologies**

AI-based risk assessments will integrate with other emerging technologies like blockchain, enhancing the accuracy and reliability of audits. Blockchain's immutable ledger, combined with AI's analytical power, can create highly secure and transparent auditing processes.

➢ **Improved Decision-Making**

AI-driven insights will enhance decision-making processes in forensic auditing. By providing a deeper and more accurate understanding of risks, AI can help auditors and stakeholders make informed decisions, ultimately improving organizational resilience and integrity.

XI. KEY FINDINGS

➢ **Role Transformation of Auditors**: AI changes the role of auditors from reviewers to interpreters of AI system results. They need to use data visualization techniques to present the findings to stakeholders.

➢ **Efficiency and Accuracy Enhancement**: AI, with its advanced analytics and natural language processing capabilities, can process networks of related parties, unstructured data, and customer activity over time more efficiently. This leads to improved trade compliance and streamlining of time-consuming, manual processes. AI also allows for the analysis of thousands of transactions over multiple fiscal years within a significantly reduced timeline, improving the efficiency of forensic audits.

➢ **Risk Assessment Improvement**: AI assists auditors in assessing risks by analyzing high volumes of data and guiding them towards areas that demand scrutiny. This strategic allocation of resources optimizes auditing efforts, leading to more focused and effective audits.

➢ **Fraud Detection**: AI has emerged as a useful tool in dissecting financial data over multiple years to identify spending patterns and high-risk transactions for a CPA to review. This is an alternative to the traditional sampling methodology used by auditors.

➢ **AI Integration in Forensic Auditing**: The paper recommends integrating AI in digital forensics operations while respecting moral and ethical principles. This results in quicker, more accurate findings and improved offender detection.

➢ **AI Auditing Frameworks:** The utilization of AI auditing frameworks such as COBIT, COSO, and IIA Artificial Intelligence Auditing Framework can encourage accountability and ensure that digital domains remain safe.

XII. RECOMMENDATIONS

❖ **Incorporate Automated Measurements:** AI used to incorporate automated measurements in risk assessment systems to improve the accuracy of predicting expected outcomes and to verify that the actual values match the predictions.

❖ **Multi-Stakeholder and Complex Governance Approach:** As the use of data and AI systems becomes crucial to core services and business, it increasingly demands a multi-stakeholder and complex governance approach.

❖ **AI Auditing:** AI auditing is the research and practice of assessing, mitigating, and assuring an algorithm's safety, legality, and ethics. It involves assessing a system, mapping out its risks in both its technical functionality and its governance structure, and recommending measures taken to mitigate these risks.

❖ **Data-Driven Approach**: AI can help auditors identify high-risk areas that require scrutiny during the audit. AI-powered predictive models can forecast financial outcomes, helping auditors assess the reasonableness of management's projections and identify potential financial issues in advance.

❖ **Forensic Skills**: For internal or external auditors, the ability to assemble the forensic skills to analyze and assess AI and its conformance to required standards is crucial. Teams targeting AI solutions require advanced knowledge of data and computer sciences, machine and deep learning.

❖ **Forensic Perspective**: Having a forensic perspective (e.g., searching for fraud regardless of its magnitude, bearing in mind that things are not always as they appear, and assuming that fraud is possible even in the presence of strong internal controls) may be helpful in developing fraud risk assessments and designing audit procedures that are responsive to assessed fraud risk.

❖ **Early Detection of Risks**: Internal audit and risk assessment are critical for the early detection of risks that arise in the processes of businesses that are becoming

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

more complex and exposed to external factors due to digitalization.

XIII. FUTURE RESEARCH

❖ **Improved Risk Assessment and Prediction:**

AI can improve the accuracy of risk assessments by incorporating automated measurements in AI-based systems. This can enhance the precision of predicting expected outcomes and instantaneously verify that the actual values match the predictions. AI can also make predictions about future risks and events by reviewing and analyzing historical transaction data.

➢ **Enhanced Efficiency and Effectiveness**:

AI can significantly benefit risk assessment by allowing auditors to perform sophisticated analyses of a client's data, guiding them towards areas that demand scrutiny. AI can also dissect financial data over multiple years to identify spending patterns and high-risk transactions, improving the efficiency of forensic audits.

➢ **Regulatory Compliance:**

AI auditing can help future-proof systems against regulatory changes. **The EU AI Act,** for example, will require conformity assessments to ensure that high-risk systems are meeting the obligations imposed on them.

➢ **AI in Digital Forensics**:

AI's role in digital forensics expected to grow, with research and developments underway to mitigate limitations and enhance performance efficiency. AI used to detect illicit activities in cryptocurrency transactions and apply statistical algorithms and machine learning techniques to identify the likelihood of future outcomes.

XIV. CONCLUSION

In conclusion, AI-based risk assessments in forensic auditing are set to transform the way audits conducted, shifting from a traditional, manual approach to a more sophisticated, data-driven methodology. The combination of AI's predictive capabilities, its ability to analyze vast amounts of data quickly, and its potential in fraud detection, promises to enhance the efficiency, accuracy, and comprehensiveness of audits. Moreover, AI's capacity to ensure regulatory compliance provides an added layer of security for organizations. However, the successful integration of AI into forensic auditing will necessitate continuous research, development, and refinement to meet evolving challenges and maximize its

@2024 International Council for Education Research and Training
ISSN: 2959-1376
2024, Vol. 03, Issue 04, 100-128
DOI: https://doi.org/10.59231/SARI7750

potential benefits. The future of forensic auditing, thus, lies in the effective harnessing of AI technology, marking a significant milestone in the field of audit and risk assessment.

REFERENCE:

1. Review of artificial intelligence (AI) for audit forensic accounting and valuation – A strategic perspective – ASOSAI journal. *Asian Journal of Government Audit*. Office of the Comptroller and Auditor General of India (CAG), Government of India (Author: Mr. Ahad Alotaibi, IT Auditor, State Audit Bureau of Kuwait). https://asosaijournal.org/review-artificial-intelligence-for-audit-forensic-accounting-and-valuation-a-strategic perspective/#:~:text=By%20leveraging%20AI%20technologies%20and,in%20th

2. AI for risk assessments from ISACA (Information Systems Audit and Control Association).https://www.isaca.org/resources/news-and-trends/industry-news/2023/can-ai-be-used-for-risk-assessments

3. Fraud detection using neural networks – A case study of income tax. MDPI-Multidisciplinary Digital Publishing Institute. https://www.mdpi.com/1999-5903/14/6/168

4. Forensic Auditing Guide; Author: Tim Vipond https://corporatefinanceinstitute.com/resources/accounting/what-is-a-forensic-audit/

5. Kumar, S. (2023). Artificial Intelligence Learning and Creativity. *Eduphoria*, *01*(01), 13–14. https://doi.org/10.59231/eduphoria/230402

6. Majji, M. (2024). Role of artificial intelligence in education. *Shodh Sari-An International Multidisciplinary Journal*, *02*(01), 33–38. https://doi.org/10.59231/edumania/9016

Received on May 30, 2024
Accepted on Aug 12, 2024
Published on Oct 01, 2024