DOI: 10.55643/fcaptp.6.53.2023.4215

APPLICATION OF ECONOMIC AND MATHEMATICAL MODELLING TO DETECT AND PREVENT FRAUD IN FINANCIAL STATEMENTS

Olena Akimova
D.Sc. in Economics, Associate Professor, Head of the Department of Accounting, Taxation and Economic Security, Donbas State Engineering Academy, Kramatorsk, Ukraine;
e-mail: kimolen1968@gmail.com
ORCID: 0000-0001-8098-1790
(Corresponding author)

Volodymyr Ivankov
PhD in Economics, Director, Forensic Research Institution, Kyiv, Ukraine;
ORCID: 0000-0001-5513-4290

Iryna Nykyforak
PhD in Economics, Associate Professor of the Department of Accounting, Analysis and Audit, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine;
ORCID: 0000-0003-4951-8073

Ruslana Andrushko
PhD in Economics, Associate Professor of the Department of Accounting and Taxation, Lviv National Environmental University, Dublyany, Ukraine;
ORCID: 0000-0003-1235-4511

Roman Rak
PhD in Economics, Associate Professor of the Department of Finance, Taras Shevchenko National University of Kyiv, Ukraine, Kyiv, Ukraine;
ORCID: 0000-0002-9526-1734

Received: 13/10/2023
Accepted: 17/12/2023
Published: 31/12/2023

ABSTRACT

This article addresses the significant challenges posed by financial statement fraud, which threatens both individual organizations and the global financial markets. It critically examines the inadequacies of traditional fraud detection methods in confronting increasingly sophisticated fraud schemes. The study focuses on the innovative use of Markov models to understand and predict the evolving nature of financial fraud risk.

The research introduces an advanced technique for adjusting the temporal evolution of Markov model transition probabilities, incorporating external factors like economic trends and regulatory changes. This recalibration employs a conditional probability function, enabling the model to remain responsive to the vicissitudes of the financial milieu. This approach allows the model to adapt to the changing financial environment. Key findings demonstrate the model's ability to evolve, reflecting the dynamic nature of financial fraud risk. A salient feature of this model is its attainment of a steady-state distribution, allowing for the ascertainment of enduring risk levels associated with financial fraud. This attribute gains prominence in environments characterized by diverse fraud detection capabilities The model achieves a steady-state distribution, indicating long-term financial fraud risk levels across various scenarios.

The paper concludes that Markov models are vital in modern financial risk management, with practical applications in areas such as credit scoring and insurance claims. It highlights the regulatory significance of these models in assessing the impact of financial regulations. Furthermore, the integration of data analytics and machine learning is explored, enhancing the models' capability against complex cyber fraud. The adaptability and predictive accuracy of these models are crucial in dynamic financial environments, necessitating continuous refinement and integration with emerging technologies and theories.

Keywords: financial fraud, Markov models, Fraud detection, Risk management, Data analytics, financial markets, Economic Trends, Regulation

JEL Classification: C02, G20, M40

INTRODUCTION

In an era where financial scandals frequently headline news stories, the imperative to detect financial statement fraud has never been more pressing. The complexities of modern financial systems, coupled with ingenious methods of deception, pose significant challenges to stakeholders striving to uphold integrity and transparency in financial reporting. Financial fraud has far-reaching implications, affecting not only individual companies but also shaking investor confidence and impacting global markets. The collapse of Enron and the 2008 financial crisis serve as stark reminders of the devastating consequences of unaddressed financial misdeeds. In this dynamic landscape, traditional methods of fraud detection often struggle to keep pace, necessitating innovative approaches to identify and mitigate risks effectively.

Financial fraud tactics have become more sophisticated and difficult to detect as the financial environment evolves with greater digitization and complicated worldwide links. The introduction of technology such as blockchain and cryptocurrency opens up new opportunities for financial deception, putting existing legal and detection mechanisms to the test. This changing environment necessitates new and adaptive techniques for fraud detection that can keep up with the financial world's fast changes and complexities. Our work recognizes these increasing issues and endeavours to overcome them through the use of advanced mathematical modelling.

There is sometimes a mismatch between theoretical fraud detection models and their practical implementation in the real, often chaotic world of finance. The diversified nature of financial fraud, which can vary from simple misstatements to intricate schemes involving several businesses and jurisdictions, exacerbates this imbalance. Our essay aims to overcome this gap by giving a model that is not only theoretically sound but also adaptive and applicable to real-world settings. We hope to contribute to a more effective and responsive framework for financial fraud detection, one that can handle both present and future demands.

This paper describes a unique use of Markov chain models for the detection of financial statement fraud. Our research sheds light on the dynamic nature of financial fraud and the efficiency of various detection tactics by modelling diverse scenarios, ranging from perfect detection environments to ones with severe restrictions. This work is significant because it has the potential to enlighten and improve the procedures used by auditors, regulatory agencies, and financial analysts in detecting and preventing financial fraud. We begin by outlining the Markov chain model and its adaptation to financial fraud detection. Various scenarios, including standard conditions and those with limited detection capabilities, are explored to demonstrate the model's adaptability. The results of our model under different scenarios are presented, followed by a detailed discussion of their implications in the world. The article concludes with a summary of our findings, their practical implications, and suggestions for future research in this field.

LITERATURE REVIEW

The detection of financial statement fraud has been a subject of extensive research and discussion, given its critical importance in maintaining the integrity of financial markets. Early research, such as the work of (Bell and Carcello, 2000), laid the groundwork by identifying key indicators of financial fraud, including abnormal financial ratios and sudden changes in accounting policies. Recent advancements, however, have shifted focus towards more sophisticated and technology-driven approaches, (Mohammadi et al., 2020; Fitri et al., 2019). Historically, fraud detection relied heavily on manual audits and analysis of financial statements, (Singleton and Singleton, 2010). Auditors would assess financial statements for irregularities, anomalies in financial ratios, or sudden changes in accounting policies, as indicators of potential fraud (Bell and Carcello, 2000). However, these methods often struggled to keep pace with the complexities and sheer volume of financial data in modern corporations. The advent of big data analytics and machine learning has transformed the landscape of fraud detection.

Kirkos et al. (2007), Papík and Papková (2022), Ngai et al. (2011), and Shah and Yasir (2023) have investigated the use of data mining techniques and artificial intelligence in identifying financial statement fraud. These methods use algorithms to spot trends and abnormalities in large datasets, providing a more automated and data-driven approach to fraud detection. Buriak and Petchenko (2021) recognize the historic character of accounting and its established procedures but emphasize the necessity for adaptation to modern difficulties such as digitization, sustainable development, and the effects of successive economic crises. They also highlight possible consequences for businesses that do not adjust to present economic conditions.

A thorough examination of mortgage lending in Uzbekistan is provided by (Abdullayeva and Ataeva, 2022), with special attention to the building financing fund. Their analysis, which draws from 23 sources, demonstrates the unanimity among academics about the need for balanced policies to prevent market imbalances and emphasizes the requirement for state-level mortgage lending stimulus. However, as (Redko et al., 2023) emphasize, the implementation of SMART specializations causes both national and regional economies to undergo substantial, strategic structural changes. The world economy is evolving quickly, and adjusting to it will need this transformational process. The authors suggest a novel strategy for economic growth that makes use of SMART specialization to promote more effective and long-term development. (Bushman, 2021) examines how scientific and technological breakthroughs have caused significant shifts in the world economy. It examines the intellectualization of the economy via the use of techniques like synthesis and analysis, highlighting issues including the development of worldwide intellectual services, the influence of ICT, and increased scientific activity. The research also looks at potential national differences and worker adaptation difficulties. In examining the critical role those institutional contexts play in the advancement of small and medium-sized firms (SMEs), (Deineha et al., 2021) emphasize the necessity of efficient government initiatives to promote SMEs' expansion. It talks about how these settings change SMEs and highlights how important they are to social and economic stability.

There is a growing recognition of the necessity for models that may be customized to certain sectors or regulatory frameworks. The usefulness and relevance of fraud detection models are improved by customization. Although novel techniques such as Markov models and technological developments hold promise for fraud detection, difficulties still exist. Financial fraud is complicated, including many individuals and elaborate strategies, which makes detection techniques challenging (Wells, 2017). Furthermore, legal and ethical issues that require careful attention include data privacy and the possibility of false positives (Chohan, 2019). For fraud detection algorithms to be more relevant and successful, they must also be tailored to certain sectors and legal frameworks. Aristova et al. (2020) provide a thorough analysis of European intellectual property (IP) courts with a particular emphasis on the recently established IP Court in Ukraine. It compares Ukrainian court developments with those of established courts in Germany, Switzerland, France, and the United Kingdom while examining their legal, organizational, and economic foundations. The research promotes socially and economically conscious judicial handling of intellectual property matters while highlighting the legal underpinnings, jurisdiction, and judge selection procedures of the courts. It also emphasizes the significance of IP in national economies. Furthermore, (Gavrylenko, 2008) provides a thorough examination of the creation and development of small businesses in the Mykolaiiv region. It looks at these businesses' present situation and future growth prospects as well as how normative-legal support affects their financial sourcing. The article also clarifies the impact of regional policy on the establishment and growth of small and medium-sized enterprises in Mykolaiiv.

Remarkably, one of the most notorious instances of financial statement fraud is the Enron incident from the early 2000s. The intricate accounting practices of the corporation, coupled with the auditors' inability to uncover them, resulted in substantial financial losses for investors (Iren and Kim, 2023). The Indian Satyam affair exposed the years-long manipulation of the financial accounts of a large IT corporation. This instance demonstrated the necessity of effective fraud detection systems to stop such widespread deceit (Lokanan et al., 2023). The importance of organizational culture on fraud detection was made clear by Toshiba's accounting debacle in Japan. Discouragement of whistleblowing and cultural issues had a part in the concealing of fraudulent actions (Sang and Keiu, 2023; Shah and Asghar, 2023; Demetriades, and Agyei., 2022). Furthermore, in Pakistan's intricate market, Khan et al. (2021) explore the influence of consumer perceptions on brand reputation. It emphasizes how important it is to foster trust among employees and make thoughtful use of PR and advertising to improve brand recognition. The biggest bankruptcy in US history resulted from accounting problems connected to the WorldCom case in the early 2000s. The inability to identify these anomalies brought attention to the necessity of more effective fraud detection systems (Petra and Spieler, 2020). The Volkswagen emissions scandal exposed the manipulation of emissions data by a large carmaker to comply with regulatory requirements. It took forensic accounting and sophisticated data analysis to find such dishonest activities (Jung and Sharon, 2019). The German Wirecard crisis revealed a multibillion-dollar fraud operation, casting doubt on the efficacy of auditing and regulatory monitoring. The case highlighted the importance of impartial and watchful fraud detection (Orlandi, 2022; Cambien et al., 2022). A few of the difficulties in detecting financial statement fraud are the complexity of fraudulent schemes and the requirement for real-time surveillance (Wells, 2017). Careful navigation is needed to ensure regulatory compliance and ethical issues, such as data privacy and the possibility of false positives.

It is only recently that Markov models have been used to identify financial fraud. According to (Norris, 1998), these models have well-established mathematical foundations, but the world of finance is just beginning to use them. Recent research has started to investigate the possibility of using Markov models to anticipate financial fraud, as demonstrated by the works of (Kirelli et al., 2020; Srivastava et al., 2008; Rajendran et al., 2023). This method takes into account the dynamic character of fraud, in which risk levels fluctuate in response to a range of variables, such as shifting economic situations and legislative changes. It makes it possible to simulate various situations, which improves our comprehension of long-term fraud risk. According to Svetlozarova Nikolova (2023), financial fraud frequently involves several organizations and cross-border transactions, making it extremely complicated. This intricacy poses serious difficulties for detection techniques, such as Markov models. Markov models have drawn interest in the realm of financial fraud detection due to their probabilistic character and capacity to capture sequential relationships.

The literature on financial fraud detection shows a progression from increasingly complex, data-driven techniques to more audit-based, classical procedures. In this regard, Markov models—which provide a dynamic and probabilistic view of fraud risk—represent a notable breakthrough. However, there are still issues to deal with, such as the intricacy of financial crime and the requirement for regulatory compliance. As these issues are addressed, future research must keep coming up with novel solutions to make fraud detection techniques both morally and practically sound. The incorporation of cutting-edge technology like blockchain, which may provide transparent and unchangeable financial data, should be the subject of future study (Lessmann et al., 2015). Furthermore, tailoring fraud detection algorithms to particular sectors and legal frameworks might increase their efficacy (Ding et al., 2019; Kumar et al., 2018). In conclusion, thanks to new modelling techniques like Markov models and significant technology developments, financial statement fraud detection has significantly changed. Effective fraud detection is crucial, as demonstrated by real-world instances, and problems demand ongoing innovation and customization in the industry. By examining the flexibility and efficiency of Markov models in tackling contemporary problems in financial statement fraud detection, this paper adds to the continuing conversation.

AIMS AND OBJECTIVES

The primary aim of this article is to conduct a comprehensive analysis of approaches to detect financial statement fraud, addressing current challenges and prospects for improvement. To achieve this overarching aim, the following specific objectives have been defined:

- to critically review traditional methods of financial statement fraud detection and explore modern technological advancements, including data analytics and machine learning, in fraud detection;
- to examine the applicability of Markov models in the context of financial statement fraud detection, considering their probabilistic nature and potential to capture dynamic risk evolution;
- to conduct scenario analysis using Markov models to evaluate the effectiveness of fraud detection under various conditions, ranging from ideal detection scenarios to scenarios with limitations and challenges;
- to discuss the policy implications of the findings, highlighting the need for adaptable and data-driven fraud detection strategies in the financial industry;
- to underscore the significance of this work in shaping the future of fraud prevention, providing insights into the potential and limitations of advanced modelling techniques in addressing contemporary fraud challenges.

METHODS

A Markov process, or Markov chain, is a stochastic process that models the probabilities of various states and how transitions occur between these states. The fundamental property of a Markov process is that the future state depends only on the current state and not on the sequence of events that preceded it (Hamilton, 1994). This is known as the Markov property or memory lessness. The transition matrix is a key component in Markov processes. It is a square matrix that describes the probabilities of moving from one state to another in a single time step. If we consider a Markov process with n states, the transition matrix P will be an $n \times n$ matrix, where each element p_{ij} represents the probability of moving from state $i\ to\ state\ j$.

The transition matrix *P* is defined as:

$$\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ p_{n1} & p_{n2} & \ddots & p_{nn} \end{bmatrix}$$

Where p_{ij} *represents the probability of transitioning from state* $\mathbf{i}$ $to\ state$ $\boldsymbol{j}$. *Each pij satisfies* $\mathbf{0} \le p_{ij} \le \mathbf{1}$. *The sum of each row* $\sum_{j=1}^{n} p_{ij}$ *signifies that the sum of the elements in each row, indexed by* $j, is\ equal\ to\ 1,$ (Kemeny and Snell, 1960).

Evolution Over Time

The state of the system at any given time $\boldsymbol{t}$ can be represented by a probability vector $\boldsymbol{v}(\boldsymbol{t})$, where each element of the vector represents the probability of the system being in a particular state at time $\boldsymbol{t}$. If $\boldsymbol{v}(\mathbf{0})$ represents the initial state probabilities, the state probabilities at a later time $\boldsymbol{t}$ can be computed as:

$$v(t) = v(0) \times P^t$$

Where, P^t *represents the transition matrix* $\boldsymbol{P}$ *raised to the power of* $\mathbf{t}$, *indicating the cumulative effect of the transition probabilities over* ***t*** *time steps.*

The operation $v(0) \times P^t$ involves matrix multiplication. This formula allows for the calculation of the probability distribution of states at any future time **t** based on the initial state probabilities and the transition probabilities defined in $\boldsymbol{P}$, (Norris, 1998; Shah and Shah, 2023). This overview provides a comprehensive insight into the Markov process transition matrix methodology, a tool widely applicable in numerous fields, including financial fraud detection. In detecting financial statement fraud, Markov chains can model how the financial status of a company may shift from one state to another (e.g., from solvent to fraudulent). Understanding these transition probabilities helps in identifying patterns and relationships among various financial indicators, thereby predicting fraudulent activities.

RESULTS

Generalized Framework for the Markov Model in Financial Fraud Detection

The state space is defined as $S = \{s_1, s_2, \ldots, s_n\}$ represent the state space of the Markov model, where each s_i corresponds to a specific risk level or category relevant to financial fraud (e.g., 'Low Risk', 'Moderate Risk', 'High Risk', etc.).The transition matrix P is an $n \times n$ matrix where each element p_{ij} represents the probability of transitioning from state s_i to state s_j . For P to be a valid stochastic matrix, each p_{ij} must satisfy two conditions i.e., Non-negativity: $0 \leq\ p_{ij}\ \leq 1\ for\ all\ i, j.$ Row Sum to One: $\sum_{j=1}^{n}\ p_{ij}$ for all i. This ensures that the probabilities for leaving any given state sum up to 1.

In the third step, we have introduced dynamic adjustment into the model with a vector θ_t, representing external factors at time t. Afterwards, transition probabilities are modified based on these factors, using a function f, such that $p_{ij}\,(t) = f(\,p_{ij}\,, \theta_t)$. This is a form of conditional probability where the condition is the external factor vector. Define f as a function that ensures the output lies within the range $[0,1]$, respecting the probability constraints. The function f takes into account various external factors like economic indicators, market volatility, or regulatory changes. The idea is that these factors can significantly influence the likelihood of a state transition in the context of *financial fraud.* Our function can be defined as $f(x) = \frac{1}{1+e^{-k(x-x_o)}}$. In our context, x could be a linear combination of p_{ij} and elements of θ_t, with k and x_o being parameters to control the steepness and midpoint of the curve, respectively. The adjusted probability $p_{ij}\,(t)$ can be given as: $p_{ij}\,(t) = \frac{1}{1+e^{-k(p_{ij}\sum m\theta_{tm}-x_o)}}$Here, $\sum m\theta_{tm}$ represents the sum of external factors, each possibly weighted to reflect their relative importance.

Then we incorporated a set of weights corresponding to different financial indicators and adjusted the transition probabilities to reflect the significance of each indicator. If $W = \{w_1, w_2, \ldots, w_n\}$, then adjust p_{ij} to $p_{ij}\,'$ using a function g, where $p_{ij}\,' = g(\,p_{ij}\,, W)$. The function g modifies p_{ij} based on the financial indicator weights in W. This is represented as a weighted sum or other mathematical formulation that takes into account the influence of each financial indicator. Furthermore, we have exemplified *g* as a function that modifies the transition probability based on the weighted significance of various financial indicators. Each weight w_i in W represents the influence of a particular financial indicator. The function g aggregates these influences to adjust the transition probability, ensuring that more significant indicators have a greater impact on the probability. For simplicity, the linear form of $g(\,p_{ij}\,, W) = \alpha\, p_{ij}\, + \sum_{k=1}^{n} w_k\, \cdot I_k$. Here, I_k are the financial indicators (e.g., cash flow, debt ratio), and α is a scaling factor for the base probability. The final adjusted probability $p_{ij}\,'$ might need normalization to ensure it remains a valid probability. After adjustments, the probabilities in each row of the transition matrix should sum up to 1. This can be achieved by applying a normalization step:

$$p_{ij}^{norm} = \frac{p_{ij}\,'}{\sum_{j=1}^{n}\, p_{ij}\,'}$$

p_{ij}^{norm} *is the normalized probability, ensuring the row sums to 1.*

Time-dependent evolution is presented through the probability distribution across states at time t, represented by $\vec{v}$(t) evolves as $\vec{v}(t+1) = \vec{v}(t)\ \times\ P^t$ (where P^t is the $t-th$ power of the transition matrix by using the Chapman-Kolmogorov equation, a fundamental property in Markov chain theory. If $\vec{v}$(0) is the initial state distribution, then $\vec{v}$(t) at any time t is given by $\vec{v}(\mathrm{t})\ = \vec{v}(0)\ \times P^t$.

Proof Using Chapman-Kolmogorov Equation,

- assume an initial state distribution $\vec{v}$(0);
- the probability distribution after one step is given by $\vec{v}(1) = \vec{v}(0) \times P$;
- applying the transition matrix repeatedly, the distribution after t steps is the result of multiplying $\vec{v}(0) \times P$(t) times: $\vec{v}(\mathrm{t}) = \vec{v}(0) \times P \times P \ldots \times P$ Simplified, this becomes $\vec{v}(\mathrm{t}) = \vec{v}(0) \times P^t$;

- Chapman-Kolmogorov Equation states that the probability of transitioning from state i to state j in t steps is the sum of the probabilities of transitioning from state i to some intermediate state k and then from k to j over all possible intermediate states k. Mathematically, it is expressed as: $p_{ij}^{t} = \sum_{k=1}^{n} p_{ik}^{(r)} . p_{kj}^{(t-r)}$for any $0 < r < t$. This aligns with the matrix multiplication in the iterative process. This concept is fundamental in predicting future state distributions in various applications, such as financial fraud detection in Markov models.

The long-term behaviour of a Markov chain is characterized by its steady-state or equilibrium distribution, where the probabilities stabilize over time, irrespective of the initial state distribution. Finally, long-term behaviour is investigated by examining $\lim_{t\to\infty} \vec{v}(\mathrm{t})$ to understand the steady-state probabilities, which can indicate the long-term risk levels of financial fraud. The long-term behaviour of the Markov chain is analyzed by examining the steady-state or equilibrium distribution. The steady-state distribution $\vec{v}$ is found by solving $\vec{v} = \vec{v} \times P$, which is a system of linear equations. In matrix terms, it's finding the eigenvector of P corresponding to the eigenvalue 1.

Proof Using Eigenvector and Eigenvalue Concept:

- in matrix terms, finding the steady-state distribution is equivalent to solving the eigenvalue equation for $P \times \vec{v}^{T} = \lambda \times \vec{v}^{T}$ For the steady-state, we are interested in the eigenvalue $\lambda = 1$;
- *Solving for* $\vec{v}$: Rewrite the equation as: $(P - I) \times \vec{v}^{T} = 0$ Here, I is the identity matrix. This equation represents a system of linear equations;
- *Normalization Constraint*: Additionally, the elements of $\vec{v}$ must sum to 1, as they represent probabilities. So, we have the constraint: $\sum_{I=1}^{n} v_i = 1$

In the context of financial statement fraud detection, the steady-state distribution $\vec{v}$ represents the long-term risk probabilities for different fraud states. For instance, if $\vec{v}$has a high probability in a 'High Risk' fraud state, it indicates a tendency towards high fraud risk over time. Understanding the steady-state distribution is crucial in assessing long-term risks and can inform decision-making processes in financial monitoring and regulation.

Defining States Relevant to Financial Fraud

In a Markov model, states represent the various conditions or scenarios that the subject (in this case, a company or financial entity). For financial fraud detection, these states should be carefully defined to reflect different levels or types of fraud risk. Examples of such states could include:

- *Low Risk:* Indicators suggest a very low probability of fraudulent activity;
- *Moderate Risk:* Certain warning signs are present, but not conclusive evidence of fraud;
- *High Risk:* Strong indicators or evidence of potentially fraudulent activity;
- *Under Investigation:* The company is currently under investigation for potential fraud;
- *Fraud Confirmed:* Fraud has been detected and confirmed.

Transition Probabilities Based on Financial Indicators

The next step is to determine the probabilities of transitioning from one state to another. This is where financial data and indicators come into play. Transition probabilities are estimated based on historical data of known fraud cases and financial trends. For example: A company with consistent and healthy financial ratios might have a high probability of staying in the "Low-risk" state. A sudden drop in cash flow, unexplained discrepancies in financial statements, or other red flags might increase the probability of moving from "Low Risk" to "Moderate Risk" or even "High Risk".

In a Markov process, the system is described by a set of states. For financial fraud detection, these states could have various levels of fraud risk (e.g., Low, Moderate, High). The transition probabilities between these states are represented in a matrix called the transition matrix.

A simulated dataset comprising financial factors such as cash flow, revenue growth, audit views, and market circumstances has been created for us. This dataset attempts to replicate as much real-world financial data as possible. Next, we have computed the transition probabilities for every state using the simulated data. The observed changes in the financial variables included in the dataset provide the basis for deriving these probabilities.

Table 1. Financial Risk State Transition Matrix (Original).

	Low Risk	**Moderate Risk**	**High Risk**
Low Risk	0.7	0.2	0.1
Moderate Risk	0.3	0.4	0.3
High Risk	0.1	0.3	0.6

There's a 70% probability that a low-risk state will remain low-risk in the next period depicted in Table 1. While there’s a 20% probability that a low-risk state will transition to a moderate-risk state. There’s a 10% probability that a low-risk state will transition to a high-risk state. We have validated the model by testing it against a separate set of data or known cases of financial fraud. The accuracy of the model is determined by how well the predicted states match the actual observed states. Then this model is updated with new financial data to maintain its accuracy and relevance. This involves recalculating the transition probabilities to reflect changes in the economic environment or market conditions.

Table 2. Financial Risk State Transition Matrix (Updated).

	Low Risk	**Moderate Risk**	**High Risk**
Low Risk	0.6	0.3	0.1
Moderate Risk	0.2	0.5	0.3
High Risk	0.1	0.2	0.7

The probability of staying in the low-risk state in Table 2 decreased to 60%. The probability of transitioning from low to moderate risk increased to 30%. The probability of transitioning from low to high risk remained the same at 10%. The values in the matrix represent the likelihood of moving from one risk state to another over a specific period. These matrices are essential to Markov chain models and help comprehend the dynamics of risk transitions. Shifts in the underlying financial circumstances or market environment are indicated by changes in the transition probabilities in the updated matrix. These matrices are useful for financial organizations to evaluate and control risks, particularly when it comes to anticipating and stopping fraudulent activity. The model's ability to adjust to shifting economic conditions and increase forecast accuracy over time is facilitated by regular changes to the transition matrix. Credit card issuers, for instance, use these models to identify anomalous transaction patterns that could point to fraud.

Scenario Setup

We have considered four states for the Markov model, State 1: Low Risk of Fraud; State 2: Moderate Risk of Fraud; State 3 is High Risk of Fraud and State 4 is Fraud Detected Assume an initial transition matrix based on data as in the Table 3.

Table 3. Fraud Risk Evolution Markov Model: Dynamics and Transitions - Initial Transition Matrix.

	Low Risk	**Moderate Risk**	**High Risk**	**Fraud Detected**
Low Risk	0.70	0.20	0.05	0.05
Moderate Risk	0.10	0.60	0.20	0.10
High Risk	0.05	0.15	0.50	0.30
Fraud Detected	0.00	0.00	0.00	1.00

There's a 70% probability that a system in a low-risk state will remain low-risk in the next period as depicted in Table 3. While a 20% probability that a system in a low-risk state will transition to a moderate-risk state and a 5% probability that a system in a low-risk state will transition to a high-risk state. There's a 5% probability that a system in a low-risk state will transition to a state where fraud is detected. Fraud Detected State (1.00 in the last column): If fraud is detected, the system will stay in the "Fraud Detected" state with a 100% probability, representing an absorbing state where once fraud is detected, the system remains in that state.

Initial State Distribution $\vec{v}(0)$: Assume the company starts with a low risk of fraud:

$$\vec{v}(0) = [1,0,0,0]$$

For long-term analysis, we have calculated $\vec{v}(\mathrm{t})$ for a large data t (e.g., t=50) to approximate the steady-state distribution and utilized the iterative multiplication, $\vec{v}(\mathrm{t}) \ = \vec{v}(0) \ \times P^t$.

In adjusting for external factors, we have supposed new regulations increase the scrutiny on financial reports, affecting the transition probabilities. Adjust P using a dynamic probability adjustment function to reflect this change. In our adjusted transition matrix P': Increase the probability of transitioning to 'Fraud Detected' from 'High Risk' (Table 4.).

Table 4. Enhanced Sensitivity to Fraud Detection - Adjusted Transition Matrix based on Risk States.

	Low Risk	Moderate Risk	High Risk	Fraud Detected
Low Risk	0.70	0.20	0.05	0.05
Moderate Risk	0.10	0.60	0.25	0.05
High Risk	0.05	0.10	0.50	0.35
Fraud Detected	0.00	0.00	0.00	1.00

Adjustment in High Risk to Fraud Detected (0.35): The higher likelihood of moving from a high-risk state to "Fraud Detected" indicates that the system is now more sensitive to spotting fraud while it is in a high-risk state. Effect on State at High Risk (0.50 to 0.50): Although there is still a chance of remaining in a high-risk condition, there is a greater awareness of the possibility of deception based on the redistribution of probabilities. Overall Impact: The matrix's modifications indicate a change in strategy, with a greater focus now being on spotting fraud when the system is in a high-risk situation.

Then we have assumed new financial indicators suggest increased risk (e.g., unusual revenue recognition patterns). Adjusted P again to reflect this increased risk, particularly affecting transitions to 'High Risk' and 'Fraud Detected'.

Table 5. Adapting to Increased Financial Risk - Further Adjusted Transition Matrix. P''Reflecting New Indicators.

	Low Risk	Moderate Risk	High Risk	Fraud Detected
Low Risk	0.60	0.30	0.05	0.05
Moderate Risk	0.10	0.50	0.30	0.10
High Risk	0.05	0.10	0.60	0.25
Fraud Detected	0.00	0.00	0.00	1.00

Adjustment for Increased Risk (Low Risk to High Risk): The probability of transitioning from a low-risk state to a high-risk state has increased in Table 5, suggesting that the new financial indicators have identified heightened risk conditions.

Enhanced Detection in Fraud State (0.25 to 0.25): The probability of transitioning from a high-risk state to 'Fraud Detected' has been adjusted, indicating a continued emphasis on fraud detection when the system is in a high-risk state.

Overall Effect: The further adjustments in the matrix reflect a continuous effort to adapt to changing financial conditions, with a focus on identifying potential fraud in response to increased risk signals.

Regarding Scenario 1, as shown in Table 3, The system may exhibit a slow transition over time to a steady state in which the probability settles. The conservative starting transition probabilities may cause the distribution to favour higher risk states somewhat over time, but not significantly. In the steady-state distribution in Table 4 for scenario 2, there may be a quicker movement towards the 'Fraud Detected' state due to the higher chance of moving from 'High Risk' to 'Fraud Detected'. This illustrates the effect of increased regulatory monitoring. Table 5 illustrates a more notable movement towards the 'High Risk' and 'Fraud Detected' states in scenario 3, especially if the financial indicators have a substantial impact on the transition probabilities. Over time, the steady state may indicate a significant fraud risk. Strategies for risk assessment and auditing priorities can be influenced by these findings. For instance, increased model risk could necessitate more thorough checks. Determining how regulatory modifications affect long-term fraud risk might help inform policy choices. For each of the three situations, the steady-state distributions have been calculated. With a probability of 1, the system eventually converges to the state "Fraud Detected." This implies that in normal circumstances, the probability of fraud detection becoming certain increases with time:

$$Steady - State: [0, 0, 0, 1]$$

The results from all three scenarios converge to the same steady state, indicating the eventual detection of fraud. This convergence might be due to the following reasons: The transition matrix in each scenario includes a non-zero probability

DOI: 10.55643/fcaptp.6.53.2023.4215

of moving to the 'Fraud Detected' state from other states, combined with the fact that once in 'Fraud Detected', there is no transition out of this state (absorbing state). The results could reflect a realistic scenario in the financial world where, given sufficient time and scrutiny, fraudulent activities are likely to be eventually detected. The convergence to 'Fraud Detected' underscores the importance of continuous monitoring and analysis in financial fraud detection. It suggests that vigilance and thorough investigation play crucial roles in uncovering fraud. The model assumes that once fraud is detected, the state does not change, which may not always be the case in real-world scenarios. Adaptations or refinements of the model could include post-detection states to more accurately reflect the dynamic nature of financial activities.

Scenario: Limited Detection Capability

In this scenario, we account for the limitations in current fraud detection methods, such as lack of resources, inadequate technology, or ineffective regulatory frameworks. These limitations can lead to scenarios where fraud goes undetected for extended periods or indefinitely. We have defined a new transition matrix $P_{limited}$ to represent this scenario.

Table 6. Transition Matrix for Limited Fraud Detection Capability: Challenges in Detecting and Sustaining Fraud Awareness.

	Low Risk	**Moderate Risk**	**High Risk**	**Fraud Detected**
Low Risk	0.80	0.15	0.04	0.01
Moderate Risk	0.25	0.50	0.20	0.05
High Risk	0.20	0.30	0.40	0.10
Fraud Detected	0.00	0.00	0.10	0.90

Limited Transition to 'Fraud Detected' (0.01, 0.05, 0.10): The probabilities of transitioning to 'Fraud Detected' are significantly lower across all risk states compared to previous scenarios. This indicates a reduced likelihood of detecting fraud, reflecting limitations in detection capabilities.

Small Probability of Exiting 'Fraud Detected' (0.10): There's a small probability of moving out of the 'Fraud Detected' state, representing the possibility of fraud going unnoticed after initial detection or successfully avoiding detection.

Overall Effect: The matrix reflects the challenges posed by limited detection capabilities, highlighting the potential for fraud to persist or remain undetected for extended periods.

In $P_{limited}$ the probabilities of transitioning to 'Fraud Detected' are significantly lower than in previous scenarios. Additionally, there's a small probability of moving out of the 'Fraud Detected' state, reflecting the possibility of fraud going unnoticed after initial detection or being covered up successfully. Scenario *Limited Detection Capability* presents a more nuanced view of financial fraud detection, acknowledging that in the real world, fraud detection is not always guaranteed, and its effectiveness can be influenced by various factors. This scenario emphasizes the need for continuous improvements in fraud detection methodologies, technologies, and regulatory frameworks to increase the likelihood of detecting and addressing financial fraud.

Table 7. Enhanced Transition Matrix $P_{limited}$ for Limited Fraud Detection: Dynamic Adjustments and Risk Factor Weighting.

	Low Risk	**Moderate Risk**	**High Risk**	**Fraud Detected**
Low Risk	0.80	0.15	0.04	0.01
Moderate Risk	0.25	0.50	0.20	0.05
High Risk	0.20	0.30	0.40	0.10
Fraud Detected	0.10	0.10	0.10	0.70

This matrix in Table 7 reflects a reality where even detected fraud might be obscured or not fully resolved, allowing transitions out of the 'Fraud Detected' state.

Enhanced Probability of Transitioning to 'Fraud Detected' (0.10, 0.10, 0.10): The probabilities of transitioning to 'Fraud Detected' from all risk states have increased. This adjustment reflects the reality where even detected fraud might be obscured or not fully resolved, allowing for the possibility of transitions out of the 'Fraud Detected' state.

Dynamic Probability Adjustment (0.70 in the 'Fraud Detected' row): The matrix incorporates dynamic adjustments to account for factors such as technological limitations, resource constraints, and regulatory weaknesses. The higher probability of staying in the 'Fraud Detected' state acknowledges challenges in fully resolving detected fraud.

Risk Factor Weighting: This adjustment reflects the varying impacts of different financial indicators on the probability of fraud being detected and addressed. The matrix considers the nuanced influence of risk factors in the detection and resolution process.

Time-dependent evolution is presented through the initial state,

$$\vec{v}(0) = [0.70, 0.20, 0.05, 0.05]$$

It represents a moderate initial risk profile. Then we calculated $\vec{v}(\mathrm{t}) = \vec{v}(0) \times P_{limited}^{t}$ for increasing values of t to see how the probability distribution evolves.

Long-Term Analysis for Limited Detection Capability

To find the steady-state distribution, we solve the eigenvalue problem for the transition matrix $P_{limited}$. The steady-state distribution $\vec{v}_{ss}$ is the left eigenvector of $P_{limited}$ corresponding to the eigenvalue 1, normalized so that its components sum up to 1. Then we have solved:

$$P_{limited}^{T} \cdot \vec{v}_{ss} = \vec{v}_{ss}$$

$$\sum \vec{v}_{ss} = 1$$

Table 8. The steady-state distribution $\vec{v}_{ss}$.

Low Risk	**50.56%**
Moderate Risk	25.41%
High Risk	13.58%
Fraud Detected	10.45%

The steady-state distribution $\vec{v}_{ss}$ Table 8 Limited Detection Capability scenario represents the long-term probabilities of being in each of the states ('Low Risk', 'Moderate Risk', 'High Risk', 'Fraud Detected'). The largest proportion is in the 'Low Risk' state, but significant probabilities are also associated with 'Moderate Risk' and 'High Risk' states, indicating that the system frequently resides in these states. Unlike previous scenarios, where 'Fraud Detected' was an absorbing state, here we expect to see a distribution that reflects the possibility of fraud remaining undetected or unresolved. A more distributed steady-state suggests that the risk of undetected fraud remains present over the long term. This outcome can inform strategies for continuous monitoring and improvement of fraud detection systems. It also highlights the importance of addressing systemic issues that might hinder effective fraud detection and resolution. The state distribution at the final time step (50th step) closely matches the steady-state distribution, confirming that the system has reached equilibrium. This means that over time, the probabilities of being in each state stabilize to the values found in the steady-state distribution.

DISCUSSION

The steady-state distributions calculated for the three scenarios provide insightful conclusions about the long-term behaviour of the financial fraud detection model. Each scenario results in the steady-state distribution converging to [0, 0, 0, 1], indicating that all states eventually transition to and remain in the 'Fraud Detected' state. In all three scenarios, the 'Fraud Detected' state acts as an absorbing state. Once the system enters this state, it cannot transition to any other state (as indicated by the row [0, 0, 0, 1] in the transition matrices. This design mirrors the real-world concept where, once fraud is detected and confirmed, a company remains in that state for the scope of the model. The steady-state finding implies that the system will eventually reach the 'Fraud Detect-ed' state, independent of the initial point. This result may indicate a positive assessment of the effectiveness of financial supervision and regulation, implying that any fraud will ultimately be discovered. The idea that fraud detection methods are effective over time is shown by the convergence of fraud detection. Although external variables like heightened regulatory scrutiny don't change the final result, they might hasten the shift to fraud detection. This is in line with the hypothesis that stricter laws and monitoring boost fraud detection systems' effectiveness.

DOI: 10.55643/fcaptp.6.53.2023.4215

Adjusting the model to account for financial indicators is meant to reflect more sensitive and immediate reactions to financial data. The result implies that heightened awareness and monitoring of financial indicators contribute to the eventual detection of fraud, albeit the end state remains unchanged. Our model's adaptability to different scenarios, such as standard analysis, increased regulatory scrutiny, and the impact of financial indicators, is a unique contribution to financial fraud detection literature. This approach aligns with the findings of (Schilit and Perler, 2010), who emphasize the evolving nature of financial fraud and the necessity of adaptable detection methods. This comparative approach is in line with the work of Albrecht et al. (2011), who explore how different factors contribute to the risk of financial fraud.

The last scenario, Limited Detection Capability, simulates the difficulties in detecting fraud in some real-world situations when insufficient resources, insufficient detection capabilities, or inadequate regulatory supervision let fraud go unnoticed or unaddressed. This scenario differs from others in that 'Fraud Detected' is not an absorbing condition. The possibility of reverting from "Fraud Detected" to a lower-risk level may indicate situations in which fraudulent activity is either successfully concealed or cannot be confirmed beyond a reasonable doubt. Unlike the previous scenarios where 'Fraud Detected' dominated the long-term result, the steady-state distribution in this scenario would probably show a more balanced probability dispersion over all states. This approach is better suited to scenarios in which fraud detection systems aren't flawless or in which fraudulent activity can be sufficiently sophisticated to go undetected for long periods. Offers a more thorough and accurate perspective on financial fraud detection through its expanded research utilising the Markov model framework. It draws attention to the difficulties and constraints present in the current systems and emphasizes the necessity of ongoing development and modification of fraud detection techniques and tools. This hypothetical situation serves as a reminder that in the intricate realm of financial supervision, creativity and alertness are essential for efficiently managing and reducing the danger of fraud. The research offers insightful information for risk management plans, highlighting the necessity of enhancing detection techniques and ongoing watchfulness. A review of present rules and procedures is necessary to improve fraud detection skills and lower the likelihood of financial fraud going unnoticed, as indicated by the steady-state balanced distribution.

Significant insights into the dynamic nature of financial risk and fraud detection techniques are revealed by a thorough investigation of the Markov model. Effective financial monitoring and fraud detection systems depend on a knowledge of probabilistic transitions between different states of risk and fraud, which is made clear by the use of Markov models in this sector. The model illustrates how the risk of financial fraud fluctuates over time due to a variety of factors, including market dynamics, regulatory changes, and economic indicators. Incorporating external elements and financial indicators into the transition probabilities through the use of a dynamic adjustment method is consistent with real-world scenarios where financial risk is dynamic and subject to fluctuations based on changing conditions. For example, the modification of probability in reaction to regulatory modifications represents how policy changes affect company behaviour and fraud risk in the world (Giovannelli et al., 2023).

The model's focus on the steady-state distribution offers crucial insights into the long-term risk profiles of financial entities. The convergence to a steady state, especially in the 'Fraud Detected' state, highlights the inevitability of fraud detection over time, given effective monitoring and regulatory mechanisms. This is corroborated by numerous historical cases where prolonged fraudulent activities, like those in Enron and WorldCom, were eventually detected, albeit after significant damage (Alsadah, and Al-Sartawi, 2023; Sahla, and Ardianto, 2023). The 2001 Enron scandal provides a crucial illustration of how our approach may have identified increasing risk factors. Transitional probabilities might have indicated that Enron's financial complexity and dishonest practices—such as off-balance-sheet financing and dubious accounting methods—were shifting from lower to higher risk stages. Comparably, the 2008-uncovered Bernie Madoff Ponzi scheme is another example of a situation where a Markov model may have identified the slow shift from an apparent low-risk to a high-risk and ultimately to a "Fraud-detected" state. If such a model had been developed, Madoff's consistently strong returns—despite market fluctuations—would have been an oddity. The model suggests a more scattered steady state in settings where detection skills are restricted, implying a constant danger of fraud going unnoticed. This is particularly relevant in the context of smaller firms or those in regions with less stringent regulatory oversight, where fraud might go undetected for extended periods.

The steady-state analysis reveals significant insights into the long-term implications of financial fraud risks. In scenarios with effective detection mechanisms, fraud inevitably becomes detected, echoing the assertions by Van Vlasselaer et al. (2015), on the effectiveness of vigilant fraud detection systems. These models may be used by financial organizations, including banks and credit card firms, for fraud detection and risk management. Similar probabilistic models are used, for instance, by credit card fraud detection systems to spot odd transaction patterns. However, the model recognizes its limits, especially in situations when detection power is constrained. This emphasizes how important it is to keep improving fraud detection techniques, technology, and regulatory frameworks.

In banking, Markov models are increasingly being integrated into credit scoring systems. These models can track the transition of a borrower's credit rating over time, offering insights into the probability of default, (Dessain et al., 2023; Chatterjee et al., 2023; Bitetto et al., 2023; Deng et al., 2023). For instance, the transition of a borrower's credit rating from a moderate to a high-risk category could trigger closer scrutiny or a reassessment of the loan terms. Insurance companies also use similar models to assess claims fraud. By analyzing the transition probabilities of claim states, insurers can identify patterns indicative of fraudulent activity (Beju et al., 2023). Regulators can evaluate the efficacy of financial rules by using Markov models. For example, changes in transition probabilities inside financial institutions might be used to examine the implementation of tighter regulatory measures during financial crises, such as the Dodd-Frank Wall Street Reform and Consumer Protection Act (Kress, 2023; Gupta, 2024). Such models could be used by the Financial Action Task Force (FATF), which establishes guidelines for stopping the financing of terrorism and money laundering, to comprehend how risk profiles change in response to modifications to AML/CFT (Anti-Money Laundering/Countering the Financing of Terrorism) laws (Baratki, 2023).

The integration of big data analytics with Markov models presents a significant advancement. Financial institutions can now process vast amounts of transactional data in real-time, allowing for more dynamic and accurate fraud detection models. This integration is particularly effective in detecting sophisticated cyber fraud schemes in online banking and e-commerce. Academic research continues to refine and extend Markov models in financial contexts. Journals like the "Journal of Financial Crime" and "Journal of Banking and Finance" often publish studies exploring advanced applications of Markov chains in financial risk management, (Bansal, 2023; Soltani and Abbes, 2023). Our models are useful, but they have limitations. Specifically, they cannot accurately estimate transition probabilities in quickly changing financial contexts, and they require large amounts of high-quality data. In conclusion, the use of Markov models in the identification of financial fraud provides evidence of the interaction between real-world finance and probabilistic mathematics. These models provide insightful information for strategic decision-making, regulatory compliance, and risk management. The ongoing development and integration of these models with cutting-edge technology and novel theoretical frameworks will be essential to protecting financial institutions from fraudulent activity as financial fraud schemes become more complex.

Our study adopts a revolutionary strategy for financial fraud detection by using a Markov model. This technique is especially unusual since it dynamically adapts to a range of real-world events. This adaptability is essential since financial fraud is a complicated and dynamic field. The importance of the model in the current financial landscape is highlighted by its capacity to adjust to changing conditions, such as shifting regulatory regimes or evolving financial indicators. This is in line with the conclusions of COSO's framework, which highlights the dynamic aspect of fraud risk assessment (Committee of Sponsoring Organizations of the Treadway Commission) (Dickins, et al., 2013).

Cases such as Toshiba in Japan and Satyam in India demonstrate the worldwide applicability of our concept. These examples demonstrate how systemic problems and cultural elements can affect fraud detection, which is consistent with the results of our model on various risk profiles in various contexts (Abdulfatah and Yahaya, 2022; Barkemeyer et al., 2020; Pande et al., 2020). Our findings have important ramifications for corporate governance, particularly in terms of strengthening audit and internal control systems. The importance of strong corporate governance measures in reducing fraud risks is highlighted by Beasley et al. (2010) and is reflected in our model's emphasis on reliable fraud detection systems. The research advocates for stronger regulatory frameworks and international cooperation in fraud detection, supporting the recommendations of the International Monetary Fund (IMF) and the World Bank on tackling corporate fraud (IMF, 2019). Future research could explore integrating this Markov model approach with other predictive analytics tools. Additionally, research could focus on customizing the model for specific industries or regions, considering unique risk factors and regulatory environments.

CONCLUSIONS

This study presents a comprehensive analysis of financial statement fraud detection using Markov chain models, highlighting their effectiveness in capturing the dynamic and complex nature of financial fraud. These models adeptly represent transitions between different fraud risk states, adapting to real-world changes like regulatory shifts and economic conditions. Our unique approach lies in the flexibility of Markov models to simulate various scenarios, offering insights into fraud detection in diverse situations, from ideal to challenging conditions. The steady-state distributions that these models yield offer vital information about the long-term risk profiles of organizations, pointing to the eventual discovery of fraud in a variety of contexts. This underscores the importance of continuous improvement in fraud detection methods, reflecting the evolving landscape of the financial industry.

Our work is especially pertinent to regulatory authorities, corporate governance organizations, financial analysts, and auditors. They emphasize the necessity of alertness, ongoing observation, and strategy modification to successfully identify and stop financial fraud. The study also highlights the possibility of incorporating cutting-edge technology into fraud detection systems, such as artificial intelligence and machine learning. Our model captures the complexities and difficulties that arise in real-world financial fraud detection by taking into account a variety of scenarios, including ones with restricted detection capabilities. Understanding this element is essential to realizing the shortcomings of the present systems and the necessity of systemic changes. However, the article does not shy away from addressing the limitations and challenges inherent in these models. It acknowledges the need for continuous refinement of probabilistic models and the importance of integrating them with other analytical techniques, such as machine learning and data analytics. This integration is crucial in enhancing the detection capabilities in the face of increasingly sophisticated financial fraud schemes.

Looking ahead, there are several avenues for further research and development. Future research could explore the integration of Markov models with AI and big data analytics, enhancing the predictive power and efficiency of fraud detection systems. Tailoring the model to address industry-specific fraud risks and regulatory environments could provide more targeted insights for different sectors. The research would gain significant depth if the model were expanded to include a worldwide view, taking into account different legislative frameworks and cultural aspects that affect fraud risk. To sum up, our research makes a substantial addition to the field of financial fraud detection. A flexible and enlightening tool for comprehending the intricacies of financial fraud is made possible by the special use of Markov chain models. In addition to advancing scholarly understanding, this research provides useful advice for enhancing fraud detection and prevention tactics in a financial environment that is changing quickly. Overall, the paper offers a balanced viewpoint, highlighting the benefits and possibilities of several strategies for identifying financial statement fraud while also emphasizing the necessity of further development and the fusion of disparate techniques. This all-encompassing strategy is essential for preserving.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

REFERENCES

1. Abdulfatah, L. A., & Yahaya, O, A. (2022). Can auditors reduce earnings management activities. *Review of Accounting and Finance, 22(4),* 429-442. https://doi.org/10.1108/RAF-10-2022-022x
2. Abdullayeva, M., & Ataeva, N. (2022). Mortgage lending with the participation of the construction financing fund of the Bank of the Future*. Futurity Economics & Law, 2(1),* 35–44. https://doi.org/10.57125/FEL.2022.03.25.05
3. Albrecht, K., Volz, K. G., Sutter, M., Laibson, D. I., & Von Cramon, D. Y. (2011). What is for me is not for you: Brain correlates of intertemporal choice for self and others. *Social cognitive and affective neuroscience, 6(2),* 218-225. https://doi.org/10.1093/scan/nsq046
4. Alsadah, N., & Al-Sartawi, A. (2023). Forensic Accounting and Cybersecurity: A Literature Review Paper. Artificial Intelligence, Internet of Things, and Society 5.0, 235-244. https://doi.org/10.1007/978-3-031-43300-9_20
5. Aristova,I., V., Aristova, I., Rezvorovych, K. R., Rezvorovich, K., Sydorova, E. O., Nesterchuk, L. P., ... & Kislitsyna, I. O. (2020). *Creation of an intellectual property court in Ukraine: protection of intellectual property rights in a system of economic security of a country*. http://dspace.onua.edu.ua/handle/11300/14364
6. Bansal, M. (2023). Earnings management: a three-decade analysis and future prospects. *Journal of Accounting Literature.* https://doi.org/10.1108/JAL-10-2022-0107
7. Baratki, L. A. (2023). FATF Standards and Their National Implementation. *Law Series Annals WU Timisoara, 45*. https://heinonline.org/HOL/LandingPage?handle=hein.journals/autimis2023&div=8&id=&page=
8. Barkemeyer, R., Faugère, C., Gergaud, O., & Preuss, L. (2020). Media attention to large-scale corporate scandals: Hype and boredom in the age of social media. *Journal of Business Research, 109,* 385-398. https://doi.org/10.1016/j.jbusres.2019.12.011
9. Beju, D. G., & Făt, C. M. (2023). Frauds in Banking System: Frauds with Cards and Their Associated Services. In *Economic and Financial Crime, Sustainability and Good Governance* (pp. 31-52).

Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-34082-6_2

10. Bell, T. B., & Carcello, J. V. (2000). A decision aid for assessing the likelihood of fraudulent financial reporting. Auditing: A *Journal of Practice & Theory*, *19*(1), 169-184. https://doi.org/10.2308/aud.2000.19.1.169

11. Bitetto, A., Cerchiello, P., Filomeni, S., Tanda, A., & Tarantino, B. (2023). Machine learning and credit risk: Empirical evidence from small and mid-sized businesses. *Socio-Economic Planning Sciences, 101746.* https://doi.org/10.1016/j.seps.2023.101746

12. Buriak, I., & Petchenko, M. (2021). Analysis of the dilemmas of building an accounting system for the needs of future economic management. *Futurity Economics & Law, 1(1),* 17–23. https://doi.org/10.57125/FEL.2021.03.25.3

13. Bushman, I. (2021). The development of the intellectual economy of the future: trends, challenges of the future. *Futurity Economics & Law*, *1*(3), 33–42. https://doi.org/10.57125/FEL.2021.09.25.04

14. Cambien, C., Leroy, A., & Omez, S. (2022). *Market & internal analysis of a PE firm's portfolio companies' valuation with an emphasis on ESG reporting & incorporation*. http://hdl.handle.net/20.500.12127/7210

15. Chatterjee, S., Corbae, D., Dempsey, K., & Ríos-Rull, J. V. (2023). A quantitative theory of the credit score. *Econometrica, 91(5),* 1803-1840. https://doi.org/10.3982/ECTA18771

16. Chohan, U. W. (2019). *The FATF in the global financial architecture: challenges and implications.* http://dx.doi.org/10.2139/ssrn.3362167

17. Deineha, I., Maslov, A., Potryvaieva, N., Verbivska, L., Koliadych, O. (2021). Institutional Environment Tools for Small and Medium-Sized Enterprises Development. *Estudios de Economia Aplicada, 39(3),* 4798. https://doi.org/10.25115/eea.v39i3.4798

18. Demetriades, P., & Owusu-Agyei, S. (2022). Fraudulent financial reporting: an application of fraud diamond to Toshiba's accounting scandal. *Journal of Financial Crime, 29(2),* 729-763. https://doi.org/10.1108/JFC-05-2021-0108

19. Deng, J., Ghasemkhani, H., Tan, Y., & Tripathi, A. K. (2023). Actions speak louder than words: Imputing users' reputation from transaction history. *Production and Operations Management, 32(4),* 1096-1111. https://doi.org/10.1111/poms.13913

20. Dessain, J., Bentaleb, N., & Vinas, F. (2023). *Cost of Explainability in AI: An Example with Credit Scoring Models. In World Conference on Explainable Artificial Intelligence* (pp. 498-516). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-44064-9_26

21. Dickins, D., & Fay, R. G. (2017). COSO 2013: Aligning internal controls and principles. *Issues in Accounting Education*, *32*(3), 117-127. https://doi.org/10.2308/iace-51585

22. Ding, K., Li, J., Bhanushali, R., & Liu, H. (2019). *Deep anomaly detection on attributed networks.* In Proceedings of the 2019 SIAM International Conference on Data Mining (pp. 594-602). Society for Industrial and Applied Mathematics. economic security of a country. http://dspace.onua.edu.ua/handle/11300/14364

23. Fitri, F. A., Syukur, M., & Justisa, G. (2019). Do the fraud triangle components motivate fraud in Indonesia? Australasian Accounting. *Business and Finance Journal, 13(4),* 63-72. https://doi.org/10.14453/aabfj.v13i4.5

24. Gavrylenko, N. V. (2008). Socio-economic analysis of small business in Mykolaiiv region. *Actual Problems Of Economics, 80*, 148-155. https://www.researchgate.net/publication/294372468_Socio-economic_analysis_of_small_business_in_Mykolaiiv_region

25. Giovannelli, F., Iannamorelli, A., Levy, A., & Orlandi, M. (2023). *The Bank of Italy's In-House Credit Assessment System for Non-financial Firms.* In Financial Risk Management and Climate Change Risk: The Experience in a Central Bank (pp. 107-137). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-33882-3_5

26. Gupta, J., Srivastava, A., & Alzugaiby, B. (2024). Schumpeterian creative destruction and temporal changes in business models of US banks. *International Review of Financial Analysis, 91*, 102951. https://doi.org/10.1016/j.irfa.2023.102951

27. Hamilton, J. D. (1994). *Time Series Analysis.* Princeton: Princeton University Press. ISBN:9780691042893

28. Iren, P., & Kim, M. S. (2023). How Harsh Should the Legislation Be to Prevent Financial Crimes?: Lessons After the Enron Scandal. In Concepts and Cases of Illicit Finance (pp. 37-50). IGI Global. https://doi.org/10.4018/978-1-6684-8587-3

29. Jung, J. C., & Sharon, E. (2019). The Volkswagen emissions scandal and its aftermath. *Global business and organizational excellence, 38(4),* 6-15. https://doi.org/10.1002/joe.21930

30. Kemeny, J. G., & Snell, J. L. (1960). *Finite Markov Chains.* Princeton, NJ: Van Nostrand. https://cir.nii.ac.jp/crid/1130000797989473280

31. Khan, R.U., Saienko, V., & Tolchieva, H. (2021). Dependence of the company's reputation and the quality of customer relations*. Economic Studies journal, 2,* 159-176. https://www.ceeol.com/search/article-detail?id=929552

32. Kirelli, Y., Arslankaya, S., & Zeren, M. T. (2020). Detection of credit card fraud in e-commerce using data mining. *Avrupa Bilim ve Teknoloji Dergisi, (20),* 522-529. https://doi.org/10.31590/ejosat.747399

33. Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert systems with applications, 32(4),* 995-1003. https://doi.org/10.1016/j.eswa.2006.02.016

34. Kress, J. C., & Zhang, J. (2023). *The Macroprudential Myth*. https://ssrn.com/abstract=4530708

35. Kumar, K., Bhattacharya, S., & Hicks, R. (2018). Employee perceptions of organization culture with respect to fraud–where to look and what to look for*. Pacific Accounting Review, 30(2),* 187-198. https://doi.org/10.1108/PAR-05-2017-0033

36. Lessmann, S., Baesens, B., Seow, H. V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. *European Journal of Operational Research, 247(1),* 124-136. https://doi.org/10.1016/j.ejor.2015.05.030

37. Lokanan, M. E., & Wilson-Mah, R. (2023). *Revisiting the Satyam Fraud: A Lesson in Corporate Governance*. SAGE Publications: SAGE Business Cases Originals. https://doi.org/10.4135/9781529618976

38. Mohammadi, M., Yazdani, S., Khanmohammadi, M. H., & Maham, K. (2020). Financial reporting fraud detection: An analysis of data mining algorithms. *International Journal of Finance & Managerial Accounting, 4(16),* 1-12. https://ijfma.srbiau.ac.ir/article_15385.html

39. Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of the literature. *Decision support systems, 50(3),* 559-569. https://doi.org/10.1016/j.dss.2010.08.006

40. Norris, J. R. (1998). *Markov chains.* Cambridge University Press. https://doi.org/10.1017/CBO9780511810633

41. Orlandi, T. (2022). *The Wirecard case: challenges for German and European supervision*. https://tesi.luiss.it/id/eprint/33285

42. Pande, A. S., & Kumar, R. (2020). Implications of Indian philosophy and mind management for agency conflicts and leadership: A conceptual framework. *IIM Kozhikode Society & Management Review, 9(1),* 34-44. https://doi.org/10.1177/2277975219858864

43. Papík, M., & Papíková, L. (2022). Detecting accounting fraud in companies reporting under US GAAP through data mining. *International Journal of Accounting Information Systems, 45,* 100559. https://doi.org/10.1016/j.accinf.2022.100559

44. Petra, S., & Spieler, A. C. (2020). *Accounting scandals: Enron, Worldcom, and global crossing.* In Corporate fraud exposed (pp. 343-360). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-417-120201022

45. Rajendran, S., John, A. A., Suhas, B., & Sahana, B. (2023). *Role of ML and DL in Detecting Fraudulent Transactions. In Artificial Intelligence for Societal Issues (pp. 59-82).* Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-12419-8_4

46. Redko, K., Zaletska, I., & Chyrva, H. (2023). Comprehensive modernization and innovative development of the SMART economy of the future. *Futurity Economics&Law, 3(1),* 35–43. https://doi.org/10.57125/FEL.2023.03.25.04

47. Sahla, W. A., & Ardianto, A. (2023). Ethical values and auditors' fraud tendency perception: testing of fraud pentagon theory. *Journal of Financial Crime, 30(4),* 966-982. https://doi.org/10.1108/JFC-04-2022-0086

48. Sang, L. T. K. (2023). Toshiba's Three-Way Split Signals the End of Poor Japanese Management. In *OVERCOMING CRISIS*: *Case Studies of Asian Multinational Corporations,* 81-93. https://doi.org/10.1142/9789811259340_0006

49. Schilit, H. M., & Perler, J. (2010). *Financial Shenanigans Third Edition*. McGraw-Hill. ISBN: 978-0-07-170308-6

50. Shah, S. S., & Amin, Y. (2023). On Trust Dynamics of Economic Growth. http://dx.doi.org/10.2139/ssrn.4531978

51. Shah, S. S., & Asghar, Z. (2023). Dynamics of social influence on consumption choices: A social network representation. *Heliyon.* https://doi.org/10.1016/j.heliyon.2023.e17146

52. Shah, S. S., & Shah, S. A. H. (2023). Trust as a determinant of Social Welfare in the Digital Economy. https://doi.org/10.21203/rs.3.rs-3117248/v1

53. Singleton, T. W., & Singleton, A. J. (2010). *Fraud auditing and forensic accounting (Vol. 11).* John Wiley & Sons. ISBN-13:978-0-471-78591-0

54. Soltani, H., & Abbes, M. B. (2023). The Predictive Power of Financial Stress on the Financial Markets Dynamics: Hidden Markov Model. *Journal of Economics and Finance, 47(1),* 94-115. https://doi.org/10.1007/s12197-022-09600-z

55. Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). Credit card fraud detection using hidden Markov model. *IEEE Transactions on dependable and secure computing, 5(1), 37-48.* https://doi.org/10.1109/TDSC.2007.70228

56. Svetlozarova Nikolova, B. (2023). *Cross-Border Tax Fraud as a Barrier to Sustainable Development.* In Tax Audit and Taxation in the Paradigm of Sustainable Development: The Impact on Economic, Social and Environmental Development (pp. 55-72). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-32126-9_3

57. Tiutiunyk, I., Kuznetsova, A., & Spankova, J. (2021). Innovative approaches to the assessment of the impact of the shadow economy on social development: an analysis of causation. *Marketing and Management of Innovations, 3*, 165-174. https://doi.org/10.21272/mmi.2021.3-14

58. Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems, 75,* 38-48. https://doi.org/10.1016/j.dss.2015.04.013

59. Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons. ISBN: 978-1-119-35195-5

Акімова О., Іванков В., Никифорак І., Андрушко Р., Рак Р.

ЗАСТОСУВАННЯ ЕКОНОМІКО-МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЛЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ШАХРАЙСТВУ У ФІНАНСОВІЙ ЗВІТНОСТІ

У статті розглядаються серйозні проблеми, пов’язані з шахрайством у фінансовій звітності, яке загрожує й окремим організаціям, і світовим фінансовим ринкам. У ній критично розглядаються недоліки традиційних методів виявлення шахрайства в протистоянні дедалі складнішим його схемам. Дослідження зосереджене на інноваційному використанні моделей Маркова для розуміння та прогнозування зміни природи ризику фінансового шахрайства.

Дослідження представляє вдосконалену техніку для коригування тимчасової еволюції ймовірностей переходу моделі Маркова, включаючи зовнішні фактори, такі як економічні тенденції та нормативні зміни. Це повторне калібрування використовує функцію умовної ймовірності, що дозволяє моделі залишатися чутливою до мінливості фінансового середовища. Такий підхід дозволяє моделі адаптуватися до мінливого фінансового середовища. Ключові висновки демонструють здатність моделі розвиватися, відображаючи динамічний характер ризику фінансового шахрайства. Основною особливістю цієї моделі є досягнення стаціонарного розподілу, що дозволяє визначити стійкі рівні ризику, пов’язані з фінансовим шахрайством. Цей атрибут стає помітнішим у середовищах, що характеризуються різноманітними можливостями виявлення шахрайства. Модель досягає сталого розподілу, що вказує на довгострокові рівні ризику фінансового шахрайства в різних сценаріях виявлення шахрайства.

У статті зроблено висновок про те, що моделі Маркова є життєво важливими в сучасному управлінні фінансовими ризиками з практичним застосуванням у таких сферах, як кредитний скоринг і страхові претензії. Також підкреслюється регуляторне значення цих моделей для оцінки впливу фінансового регулювання. Крім того, досліджується інтеграція аналізу даних і машинного навчання, що підвищує здатність моделей протистояти складному кібершахрайству. Адаптивність і точність прогнозування цих моделей є вирішальними в динамічному фінансовому середовищі, що вимагає постійного вдосконалення та інтеграції з новими технологіями й теоріями.

Ключові слова: фінансове шахрайство, моделі Маркова, виявлення шахрайства, управління ризиками, аналітика даних, фінансові ринки, економічні тенденції, регулювання

JEL Класифікація: C02, G20, M40