SCIENTIFIC OASIS

Decision Making: Applications in Management and Engineering

Journal homepage: www.dmame-journal.org
ISSN: 2560-6018, eISSN: 2620-0104

Decision-Oriented Framework on Detecting and Countering Finance Management Fraud Amid Big Data Times: Characteristics, Risk Assessment and Technology-Driven Countermeasures

Yilin Lv[1], Youyou Shang[2*], Qianhui Yu[3], Tianyue Zhao[4], Shuti Li[2]

1 Guangzhou College of Technology and Business
2 Ruthin school
3 Chase Grammar School
4 SSAL College

ARTICLE INFO

Article history:
Received 25 April 2025
Received in revised form 19 July 2025
Accepted 10 August 2025
Available online 05 December 2025

Keywords:
Data Control Technology, Financial Fraud, AI Fraud Detection, Decision-Oriented Framework, Internal Audit

ABSTRACT

The objective of this study was to examine how data governance maturity, artificial intelligence (AI) integration, internal audit frequency, employee training, access control robustness, and the implementation of anomaly detection systems affect the occurrence of financial fraud. The investigation focused on business organisations operating in China. The dataset consisted of 218 organisations, with each organisation serving as the unit of analysis. Data analysis was performed using RStudio with R programming, applying exploratory factor analysis and regression modelling techniques to the organisational data. The findings indicate that AI integration, employee training, and access control robustness have no significant effect on financial fraud occurrence. In contrast, data governance maturity, internal audit frequency, and the application of anomaly detection systems were found to significantly influence the incidence of financial fraud within business organisations. These results provide valuable insights for Chinese businesses aiming to reduce the likelihood of financial fraud.

1. Introduction

The rapid digitisation of financial systems has reshaped the global business landscape, positioning data as one of the most critical organisational assets [1; 69]. In the modern financial environment, enterprises increasingly rely on extensive data analytics and digital infrastructures to support decision-making, forecasting, and risk management processes [2]. Nevertheless, the growing complexity of these digital systems has concurrently heightened the exposure to financial fraud, data manipulation, and cybercrime. Financial management fraud poses a severe challenge to organisational stability, investor confidence, and overall market integrity [3]. As business operations become progressively data-driven, there is an urgent requirement for strategic frameworks that can effectively detect and mitigate fraudulent practices within financial management systems [4].

Financial fraud encompasses intentional acts of deception undertaken for financial benefit,

* *Corresponding author.*
E-mail address: kk19947683268@163.com

https://doi.org/10.31181/dmame8220251574

which can compromise corporate governance, erode investor trust, and impede economic growth [5]. In the big data era, where immense volumes of structured and unstructured financial data are constantly produced and analyzed, ensuring data security and reliability is imperative. Organizations must uphold both compliance and accountability through robust systems of data governance and risk assessment [6]. The adoption of AI, machine learning, and automated anomaly detection tools has introduced innovative opportunities for enhancing fraud prevention strategies. However, despite technological advancements, numerous firms continue to face difficulties in creating cohesive systems that integrate governance maturity, AI-based surveillance, and employee responsibility [7].

Comprehensive financial fraud detection requires an integrated approach that combines data governance maturity, internal auditing processes, employee training, and advanced technological applications [8]. Data governance maturity ensures that financial data are efficiently managed, stored, and applied within secure and transparent frameworks [9]. Organizations with higher levels of governance maturity are generally more capable of identifying irregularities and maintaining compliance standards. Similarly, the incorporation of AI and predictive analytics has proven to be a significant advancement in detecting suspicious transactions and abnormal financial behaviors [10]. These technologies enable rapid analysis of extensive datasets to identify unusual patterns that might elude traditional audit techniques [11]. Nonetheless, the effectiveness of AI-based systems depends on their strategic alignment with governance and audit mechanisms.

Internal audit frequency also represents a vital element in preventing financial fraud. Frequent audits help organizations continuously evaluate and refine their internal control systems, identify potential vulnerabilities, and address weaknesses before they result in financial losses [12]. Additionally, employee training in data ethics and cybersecurity promotes awareness and accountability, thereby minimizing the risk of human error or deliberate misconduct [13]. The ethical dimension of data management has become increasingly significant in contemporary business environments, as insider threats and inadvertent breaches account for a considerable proportion of fraud incidents [14]. Educating employees to identify fraudulent activities and comply with data protection principles strengthens the overall security of financial operations. Moreover, access control robustness and anomaly detection deployment play an essential role in curbing fraud risk [15]. Strong access controls restrict unauthorized entry into financial databases, while anomaly detection systems automatically flag irregular transactions or behavioral deviations from established benchmarks [16]. Integrating AI-based anomaly detection enhances an organisation's ability to respond swiftly to emerging financial threats [17]. Collectively, these elements support the creation of a decision-oriented framework for financial fraud management, one that integrates big data analytics, AI, and governance principles to ensure transparency, accountability, and data security.

The primary objective of this research is to assess how data governance maturity, AI integration, internal audit frequency, employee training, access control robustness, and the implementation of anomaly detection systems affect the prevalence of financial fraud in business enterprises. By examining these variables within China's digital financial context, this study provides empirical insights into the relationship between technology and managerial practices in improving fraud prevention. The research contributes to the growing body of knowledge on digital finance governance and offers practical guidance for developing technology-driven systems that protect financial integrity in the age of big data.

2. Review of Literature

In the contemporary banking sector, data holds a crucial role as it encompasses all client-related

account information and transactional records [18]. Managing such sensitive data necessitates the implementation of robust mechanisms that incorporate multiple layers of protection to minimize the risk of fraudulent activities. Nonetheless, breaches in financial data systems remain relatively common, indicating that cybersecurity frameworks and data protection measures require continuous enhancement to mitigate potential fraud risks [19]. Various software solutions and third-party assessment services are now available in the market to assist organizations in preventing data manipulation and unauthorized access, both of which can lead to fraudulent practices [20].

Despite these advancements, the effective management of financial data, including the preparation and analysis of financial statements and forecasts, remains vital to preventing financial fraud [21]. The maturity of data management systems is therefore regarded as a key determinant in reducing the likelihood of data breaches, which can otherwise have severe implications for financial security. Consequently, financial institutions must develop advanced and comprehensive fraud protection mechanisms to safeguard their data from unauthorized interference [22]. In addition, strategic improvements in data handling processes are essential, enabling organizations to strengthen their data protection frameworks and achieve a competitive advantage in risk mitigation [23]. As financial data directly informs decision-making processes, its management must be conducted with precision and care to prevent any form of fraudulent activity.

H1: There is a relationship between data governance maturity and financial fraud occurrence.

The integration of AI into financial management has become essential in contemporary contexts to enhance data protection and security [25]. Through AI-driven algorithms, organizations can strengthen data protection frameworks and develop more sophisticated layers of defense. The incorporation of self-monitoring and alert systems powered by AI enhances the efficiency of financial processes by detecting and preventing fraudulent activities while ensuring that any irregularities are promptly reported [26]. In the domain of data management, the application of AI facilitates systematic processing and oversight, ensuring that financial operations are aligned with modern technological standards [27]. The utilization of AI in financial fraud detection enables timely identification and resolution of potential risks, thereby reinforcing institutional resilience.

Moreover, when integrated with financial governance systems, AI can significantly improve risk management by generating automated alerts for unusual financial transactions or inconsistencies and forwarding these alerts to senior management for review [28]. Hence, AI plays a pivotal role in managing the financial data of organizations, serving as a crucial element in both fraud prevention and operational optimization [29]. The strategic integration of AI not only strengthens data security but also enhances the overall financial advantage derived from accurate, well-protected, and efficiently managed data.

H2: There is a relationship between the use of artificial intelligence in financial processes and financial fraud occurrence.

The frequency of internal audits serves as a crucial element in preventing fraudulent activities within financial systems [30]. To effectively mitigate such risks, organizations must establish a structured and consistent internal audit schedule that enhances the overall efficiency of fraud prevention mechanisms. Conducting timely and frequent audits contributes to the reliability and accuracy of financial records, thereby reducing the likelihood of fraudulent alterations or misstatements [31]. Internal audits play a central role in ensuring the secure management of financial data, as they help identify vulnerabilities and verify the integrity of accounting practices. These audits should be conducted at regular intervals, enabling the detection and rectification of any data breaches or irregularities [32].

Furthermore, understanding the occurrence of financial fraud is essential for developing stronger preventive measures, given that the quality and transparency of data are critical

determinants of financial integrity [33]. Audits related to financial matters must follow a well-designed framework in which all relevant information is reviewed and reported systematically. Establishing an appropriate audit frequency, approved and overseen by senior management and financial control teams, ensures greater accountability and improves the organization's ability to assess and manage financial risks effectively [34]. Consequently, a strategic approach to audit scheduling can substantially strengthen financial governance and fraud detection capabilities.

H3: There is a relationship between internal audit frequency and financial fraud occurrence.

Employee training in data management represents a fundamental component of effective financial governance [35]. When employees are well-trained and motivated, they are more capable of establishing robust mechanisms for handling financial data securely and efficiently. The human resource department holds the primary responsibility for equipping employees with the skills required to address financial management challenges and uphold organizational data integrity [36]. Properly trained employees are better prepared to identify potential breaches, respond to financial irregularities, and engage in ethical whistleblowing when misconduct occurs [37]. Furthermore, training programmes that incorporate modern AI applications and big data management practices enhance employees' technical competence and ethical awareness in managing financial data [38]. Although employees involved in data breaches are also subject to training interventions, greater emphasis should be placed on cultivating ethical behavior and accountability within the workforce, a responsibility that rests primarily with the human resource department [39]. Data management and financial integrity are critical organizational concerns, requiring continuous improvement in employee performance and ethical standards [40]. Comprehensive and well-structured training focused on financial reporting and data protection not only strengthens employees' confidence but also empowers them to detect and report any financial misconduct effectively.

H4: There is a relationship between employee training on data ethics and security and financial fraud occurrence.

The ability of employees to effectively manage and control the flow of financial data significantly enhances the operational efficiency of an organization's finance department [41]. Establishing a well-structured approach to financial information management enables institutions to address emerging financial issues more effectively and maintain accurate reporting. A high degree of control over financial data is therefore a critical factor in ensuring financial stability and mitigating risks associated with fraud or data manipulation [42]. Employee access to financial data must be appropriately regulated to ensure that fraud prevention measures remain robust and effective [43]. In this regard, the human resource department should priorities employee training by incorporating AI tools and other advanced technologies to enhance data flow control and reinforce ethical awareness in handling financial information [44]. When employees possess adequate access control skills and an understanding of secure data handling, they are better equipped to prevent breaches and maintain the confidentiality and integrity of financial information [45]. Moreover, employees must receive continuous training to address potential financial challenges that could compromise their performance or expose the organization to fraud-related risks [46]. Conversely, when financial management teams lack sufficient capability or authority to regulate data flow, the organization becomes vulnerable to unauthorized access and manipulation of financial records by fraudulent actors. Strengthening data access control and employee competence is therefore essential to safeguarding the integrity of financial systems.

H5: There is a relationship between access control strength and financial fraud occurrence.

The development and implementation of advanced software systems to regulate data flow are essential for effective financial control and oversight [47]. Organizations must address data management challenges that can undermine their operational efficiency and overall productivity.

Establishing robust data control mechanisms is therefore a critical requirement, as it enables organizations to manage information flow more effectively and minimize exposure to financial irregularities [48]. International collaboration and enhanced employee training can further support the creation of systems capable of identifying and preventing fraudulent activities [49]. By improving the efficiency and traceability of information flow, organizations can manage financial data more securely and reduce the likelihood of fraud. Financial fraud detection remains a vital organizational priority, necessitating the adoption and deployment of modern technological tools designed to identify potential threats at an early stage [50]. The integration of these advanced detection tools with AI systems, alongside comprehensive employee training, can significantly strengthen an organization's capacity to monitor and safeguard its financial operations [51]. Such integration enhances both financial management and data protection, thereby reducing the risk of fraudulent activities and reinforcing institutional resilience against financial misconduct.

H6: There is a relationship between anomaly detection deployment and financial fraud occurrence.

3. Material and Method

The population for this research comprised business organizations in China that maintain transactional systems and internal financial reporting structures. The study focused on understanding how these organizations manage digital finance operations and utilize such systems to mitigate fraudulent activities. This population was selected to examine how various organizational factors contribute to controlling financial fraud occurrences. The participating organizations were identified through the Chamber of Commerce, national business registries, industry associations, and commercial databases. Only organizations that provide internal financial services supported by digital resources were included in the study. Data were collected from Chief Data Officers (CDOs) and Chief Financial Officers (CFOs), as these individuals are responsible for overseeing information technology security, financial management, and internal audit processes. Consistent with prior research, which suggests that a sample size between 200 and 400 organizations is appropriate for organizational-level analyses, this study followed a similar range.

A Likert scale-based questionnaire was employed for data collection, with both printed and electronic versions used. In total, 353 questionnaires were distributed across China. Some were sent via email to respondents whose physical access was constrained in order to save time and reduce logistical expenses. Informed consent was obtained from all participants prior to data collection. Out of the distributed questionnaires, 233 were returned, and after removing five outliers, a final sample of 218 valid responses was used for data analysis. Statistical analyses were conducted using RStudio with R programming [61]. The data analysis process began with the identification of outliers, followed by the assessment of skewness and kurtosis, which confirmed that the data distribution was normal. The mean and standard deviation values also indicated an appropriate distribution within the sample. Since the unit of analysis for this study was the organization rather than the individual, no personal-level data were collected. Only demographic information related to the participating organizations was included, while critical or sensitive organizational details were not disclosed in this research.

4. Findings

In this study, the collected data were examined to assess the reliability of the measurement instrument used for each construct. To ensure internal consistency, Cronbach's alpha was calculated, with a minimum threshold value of 0.70 applied to confirm acceptable reliability [24]. The Cronbach's alpha results, presented in Table 1 and Figure 1, indicated that all variables achieved satisfactory reliability levels. Consequently, all constructs were deemed valid and suitable for

subsequent analysis, as the validity of each construct was empirically established. Additionally, the research assessed the coefficient of determination (R^2) to evaluate the extent to which the independent variables explained the variance in the dependent variable. The R^2 value measures how changes in dependent variables can be attributed to variations in independent variables. According to Hair et al. [24], an R^2 value above 0.19 indicates a weak effect, above 0.33 represents a moderate or substantial effect, and above 0.67 signifies a strong effect.

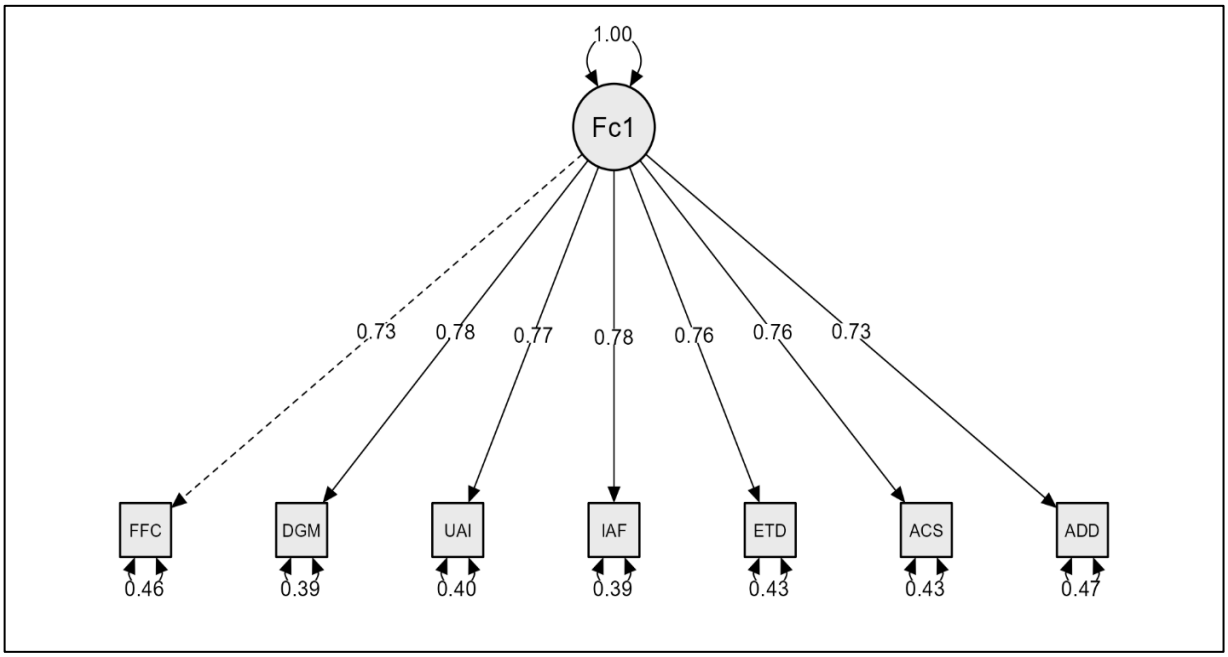

Fig.1: Model Plot

Note: FFC = Financial Fraud Occurrence, ADD = Anomaly Detection Deployment, ACS = Access Control Strength, ETDE = Employee Training on Data Ethics, IAF = Internal Audit Frequency, UAI = Use of Artificial Intelligence in Financial Processes and Data Governance Maturity

The results of this study, as reported in Table 1, revealed that internal audit frequency and employee training on data ethics demonstrated a moderate effect on financial fraud occurrence. Conversely, all other variables exhibited a strong influence on financial fraud occurrence. These findings confirm that the independent variables collectively exert a significant impact on the dependent variable.

Table 1
Cronbach's Alpha and Coefficient of Determination

Variable	Cronbach's Alpha	R^2
IAF	0.781	0.537
DGM	0.781	0.608
UAI	0.771	0.596
ACS	0.756	0.610
ETDE	0.756	0.570
FFC	0.733	
ADD	0.731	0.534

During the data analysis using exploratory factor analysis, this study examined the factor loadings of all variables. Significant factor loadings indicate that the variables are measured reliably and are suitable for assessing the hypothesized relationships. A p-value of 0.05 was applied as the threshold for determining the significance of factor loadings [24]). The results, presented in Table 2.

Table 2
Factor Loadings

Factor	Indicator	Estimate	Std. Error	z-Value	p	95% CI Lower	95% CI Upper
Factor 1	FFC	1	0	—	—	1	1
	DGM	1.087	0.097	11.24	< .001	0.898	1.277
	UAI	1.094	0.098	11.13	< .001	0.902	1.287
	IAF	1.107	0.098	11.26	< .001	0.914	1.299
	ETDE	1.060	0.097	10.87	< .001	0.869	1.251
	ACS	1.074	0.098	10.91	< .001	0.881	1.267
	ADD	1.003	0.095	10.51	< .001	0.816	1.190

As shown in Table 3, all variables in this research achieved AVE values above 0.50, indicating that the data met the required threshold for convergent validity. Consequently, convergent validity was established, confirming that the research data were reliable and appropriate for subsequent analysis.

Table 3
Average Variance Extracted

Variable	Average Variance Extracted
IAF	0.566
DGM	0.573
UAI	0.673
ACS	0.763
ETDE	0.563
FFC	0.579
ADD	0.688

The study assessed convergent validity by calculating the average variance extracted (AVE), which evaluates the extent to which the measurement instrument captures substantial variance for each construct. AVE values exceeding 0.50 are considered sufficient to confirm convergent validity [24]. Figure 2, show that all variables achieved significant factor loadings. Accordingly, the data were considered reliable and appropriate for use in this research, supporting the validity of the measurement instrument.

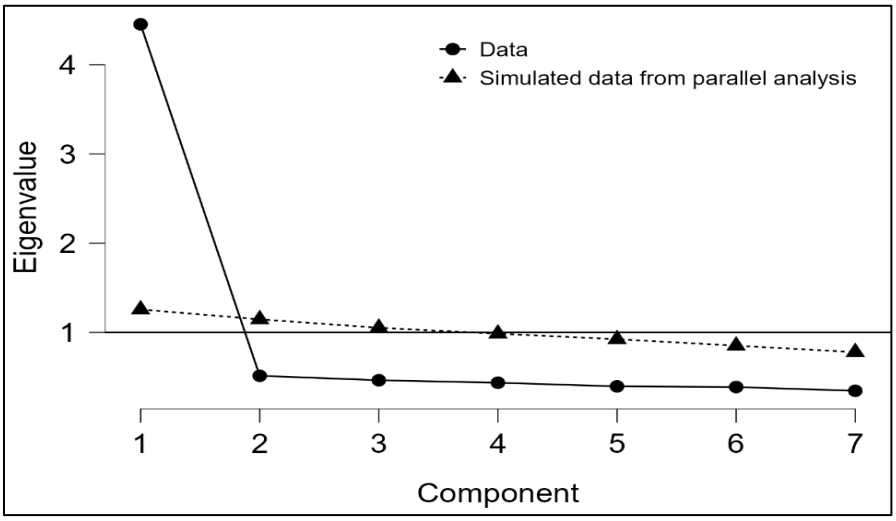

Fig.2: Scree Plot

This study further examined the residual values for each variable. In regression analysis, a residual value represents the portion of an observed variable that is not accounted for by the

model, effectively indicating the difference between the predicted and observed values. The residual values for all variables, as reported in Table 4, showed p-values below 0.001 [24]. These results confirm that the residuals are statistically significant, indicating that the model's predictions align closely with the observed data and appropriately explain the variation in the dependent variable.

Table 4
Residual Variance

Indicator	Estimate	Std. Error	z-value	p	95% CI Lower	95% CI Upper
FFC	0.566	0.062	9.161	< .001	0.445	0.687
DGM	0.502	0.057	8.728	< .001	0.389	0.614
UAI	0.532	0.060	8.807	< .001	0.414	0.651
IAF	0.515	0.059	8.712	< .001	0.399	0.630
ETDE	0.557	0.062	8.976	< .001	0.435	0.678
ACS	0.562	0.063	8.952	< .001	0.439	0.685
ADD	0.576	0.063	9.175	< .001	0.453	0.699

The hypotheses were evaluated using a t-value threshold of 1.96 to determine significance [24]. The results indicate that H1 is supported, showing a significant relationship between data governance maturity and the occurrence of financial fraud. In contrast, H2 was not supported, as no significant relationship was found between the use of artificial intelligence in financial processes and financial fraud occurrence. H3 was supported, demonstrating a significant association between internal audit frequency and financial fraud occurrence. The results for H4 indicated no significant relationship between employee training on data ethics and security and financial fraud occurrence. Similarly, H5 was not supported, as access control strength showed no significant effect on financial fraud occurrence. Finally, H6 was supported, with anomaly detection deployment exhibiting a significant relationship with financial fraud occurrence. The detailed results of the regression analysis are presented in Table 5.

Table 5
Regression

Predictor	Unstandardized Coefficient	Std. Error	Standardized Coefficient	t	p	Tolerance	VIF
DGM	0.216	0.07	0.221	3.078	0.002	0.476	2.101
UAI	0.114	0.07	0.118	1.631	0.104	0.465	2.152
IAF	0.165	0.07	0.172	2.371	0.019	0.467	2.143
ETDE	0.118	0.068	0.121	1.723	0.086	0.492	2.031
ACS	0.077	0.068	0.08	1.130	0.26	0.487	2.053
ADD	0.144	0.068	0.145	2.123	0.035	0.523	1.912

5. Discussion and Conclusion

The study analyzed the data to derive findings and achieve the research objectives. The results for H1 indicate a significant relationship between data governance maturity and the occurrence of financial fraud. These findings align with previous research, which emphasizes that robust data governance frameworks enhance fraud control mechanisms [52]. Contemporary organizations are encouraged to integrate AI technologies alongside multiple layers of governance to prevent fraudulent activities [53]. Implementing stringent data governance protocols at every stage of financial transactions is recommended, and the use of block chain technology can further strengthen fraud prevention through digital control and transparent reporting [54]. Collectively, these practices contribute to improving data control mechanisms and reducing fraud in digital financial transactions.

Regarding H2, the results indicate no significant relationship between AI utilization in financial processes and financial fraud occurrence. This contrasts with earlier studies suggesting that AI plays a key role in detecting fraudulent activities [55]. In the context of the organizations examined in this study, AI adoption appears limited, with insufficient mechanisms in place for effective utilization [56]. Consequently, organisations should enhance AI integration strategically, combining modern AI tools with financial processes to improve monitoring, reporting, and mitigation of fraudulent activities [57; 58]. The findings for H3 demonstrate a significant relationship between internal audit frequency and financial fraud occurrence. Prior research highlights that regular internal audits are critical in controlling fraud [59]. In this study, a structured routine of internal audits is recommended, potentially supported by third-party auditing teams to strengthen audit capabilities [60]. Utilizing modern technologies within internal audit processes can detect fraudulent activities more effectively and promote whistleblowing mechanisms. Regular audits ensure continuous monitoring of financial operations and support effective financial governance [62; 63].

For H4, no significant relationship was found between employee training on data ethics and security and financial fraud occurrence. Although previous studies have emphasised that employee training can reduce fraud, particularly in finance departments, the organisations in this study may have limited ethical practices for employees, which could explain the lack of effect [66; 67]. Promoting ethical conduct, providing incentives, and advancing reporting mechanisms are recommended strategies to mitigate fraud, but these appear underdeveloped in the context of the sampled organisations [68]. Similarly, H5 results indicate no significant relationship between access control strength and financial fraud occurrence. Literature suggests that strong access control supports timely and secure financial transactions [70]. However, in the organizations studied, access control systems exerted minimal influence on fraud prevention [30]. To enhance fraud mitigation, firms should integrate AI and big data tools, alongside whistleblowing systems, to complement access control measures [64; 65]. Improving access control remains essential, but it should be part of a broader, technology-enabled fraud prevention strategy.

Finally, the findings for H6 show a significant relationship between anomaly detection deployment and financial fraud occurrence. Previous research supports that deploying fraud detection mechanisms is effective in mitigating financial fraud [71]. Organizations should implement robust detection tools, potentially supported by third-party oversight, to strengthen fraud management. The effectiveness of these mechanisms is further enhanced when top management actively prioritises fraud prevention and employees are trained to use detection systems effectively [63; 68]. Without structured systems and ethical engagement from employees, managing financial control and preventing fraud becomes considerably more challenging.

6. Theoretical and Practical Implications

The findings of this study provide significant theoretical and practical contributions for both academic and professional stakeholders engaged in financial management, data governance, and corporate auditing. From a theoretical perspective, the research advances the digital finance literature by highlighting the roles of data governance maturity and internal audit frequency as critical variables within anomaly detection systems aimed at fraud prevention. By examining the relationships between data governance maturity, internal audit frequency, anomaly detection implementation, and the incidence of financial fraud, the study identifies these factors as central components of an effective fraud prevention framework. While AI adoption and employee training contribute additional value, the results indicate that the effectiveness of fraud reduction ultimately depends on an organisation’s readiness and the quality of implementation, offering opportunities for further investigation in future studies.

From a practical standpoint, the study underscores the importance of organisations actively enhancing their data governance maturity and, to a certain extent, internal audit functions. Enterprise organisations are encouraged to establish clear governance models that define data ownership, accountability, and compliance procedures, leaving minimal ambiguity. Best practices include instituting a regular internal audit cycle with periodic reviews and leveraging technology to streamline anomaly identification and fraud deterrence. Beyond detecting anomalies, organisations should integrate AI or machine learning into audit processes, enabling real-time oversight, monitoring, and fraud detection during financial transactions, thereby enhancing public trust and ensuring authorised access. Furthermore, incorporating cloud-based AI or machine learning within enterprise resource planning and financial systems can improve data quality through real-time verification, enhance accuracy, reduce errors, minimise disruptions, and increase responsiveness, representing a comprehensive approach to fraud prevention and operational excellence.

In conclusion, the study suggests that management should foster a culture of awareness and proactive fraud detection. By leveraging information to improve access controls and employing AI-enhanced technologies, organisations can conduct more effective fraud risk assessments and strengthen their governance frameworks. These findings emphasise the need for firms to be technologically advanced, maintain mature governance structures, ensure transparency, cultivate trust in their processes, optimise operational synergy, and provide continuous awareness to safeguard financial integrity in the era of big data.

7. Limitations and Future Directions

This research has certain methodological limitations that constrain the generalisability of its findings. Firstly, data were collected exclusively from business organisations in China, which limits the applicability of the results to other regional contexts. Future studies should consider collecting data from multiple countries to conduct multigroup analyses, enabling comparisons across different contexts. Such research would make a valuable contribution by enhancing the understanding of the applicability of these findings in diverse organisational and cultural settings. Secondly, this study employed a cross-sectional design, which restricts the temporal implications of the findings, as data were captured at a single point in time. Future research is recommended to adopt longitudinal approaches, incorporating time-series data from financial reports and interview-based insights. This would provide a deeper understanding of trends and changes over time, thereby enhancing the practical and theoretical significance of the findings. Furthermore, this study did not adopt a mixed-methods approach, which limits the explanatory power regarding relationships that were not supported quantitatively. Future research should consider combining survey-based data with in-depth interviews across different organisations. Such an approach would extend the body of knowledge, provide richer insights into financial fraud prevention mechanisms, and clarify the contextual factors influencing the observed relationships. Overall, employing these methodological enhancements in future studies would generate more comprehensive insights and advance scholarly understanding in this field.

References

[1] Achakzai, M. A. K., & Peng, P. (2022). Using machine learning Meta-Classifiers to detect financial frauds. *Finance Research Letters*, *48*, 102915. https://doi.org/10.1016/j.frl.2022.102915

[2] Adil, M., Zhang, Z., Jamjoom, M. M., & Ullah, Z. (2024). OptDevNet: A Optimized Deep Event-Based Network Framework for Credit Card Fraud Detection. *IEEE Access*, *12*, 132421-132433. https://doi.org/10.1109/ACCESS.2024.3458944

[3] Aljofey, A., Rasool, A., Jiang, Q., & Qu, Q. (2022). A Feature-Based Robust Method for Abnormal Contracts Detection in Ethereum Blockchain. *Electronics (Switzerland)*, *11*(18), 2937. https://doi.org/10.3390/electronics11182937

[4] Bian, L., Zhang, L., Zhao, K., Wang, H., & Gong, S. (2021). Image-Based Scam Detection Method Using an Attention Capsule Network. *IEEE Access*, *9*, 33654-33665. https://doi.org/10.1109/ACCESS.2021.3059806

[5] Cai, S., & Xie, Z. (2024). Explainable fraud detection of financial statement data driven by two-layer knowledge graph. *Expert Systems with Applications*, *246*, 123126. https://doi.org/10.1016/j.eswa.2023.123126

[6] Cai, S., Zheng, Y., Li, J., Tu, D., & Liu, H. (2025). Research on the impact mechanism of financial fraud risk among urban elderly in the context of population aging: Empirical data from China aging finance forum. *Finance Research Letters*, *77*, 107068. https://doi.org/10.1016/j.frl.2025.107068

[7] Cao, R., Liu, G., Xie, Y., & Jiang, C. (2021). Two-Level Attention Model of Representation Learning for Fraud Detection. *IEEE Transactions on Computational Social Systems*, *8*(6), 1291-1301. https://doi.org/10.1109/TCSS.2021.3074175

[8] Cao, R., Wang, J., Mao, M., Liu, G., & Jiang, C. (2023). Feature-wise attention based boosting ensemble method for fraud detection. *Engineering Applications of Artificial Intelligence*, *126*, 106975. https://doi.org/10.1016/j.engappai.2023.106975

[9] Chen, D., Wang, F., & Xing, C. (2021). Financial reporting fraud and CEO pay-performance incentives. *Journal of Management Science and Engineering*, *6*(2), 197-210. https://doi.org/10.1016/j.jmse.2020.07.001

[10] Chen, G. (2025). Intelligent recognition of financial fraud based on CART decision tree. *International Journal of Information and Communication Technology*, *26*(11), 1-20. https://doi.org/10.1504/IJICT.2025.146100

[11] Chen, H., Shi, D., Zhou, X., Zhang, M., & Liu, L. (2024). Application research of credit fraud detection based on distributed rotation deep forest. *Intelligent Data Analysis*, *28*(4), 1067-1091. https://doi.org/10.3233/IDA-230193

[12] Chen, L., Jia, N., Zhao, H., Kang, Y., Deng, J., & Ma, S. (2022). Refined analysis and a hierarchical multi-task learning approach for loan fraud detection. *Journal of Management Science and Engineering*, *7*(4), 589-607. https://doi.org/10.1016/j.jmse.2022.06.001

[13] Petrukha S , Okhrimenko V , Matsenko D . Debt policy in times of crisis: management technologies and countering singularity. Economics, Finance and Management Review, 2024(4(20)):18-29. https://doi.org/10.36690/2674-5208-2024-4-18-29

[14] Chen, W. (2024). Financial fraud recognition based on deep learning and textual feature. *International Journal of Information and Communication Technology*, *25*(1-2), 1-15. https://doi.org/10.1504/IJICT.2024.143633

[15] Chen, Y., & Wu, Z. (2023). Financial Fraud Detection of Listed Companies in China: A Machine Learning Approach. *Sustainability (Switzerland)*, *15*(1), 105. https://doi.org/10.3390/su15010105

[16] Chen, Z. Y., & Han, D. (2023). Detecting corporate financial fraud via two-stage mapping in joint temporal and financial feature domain. *Expert Systems with Applications*, *217*, 119559. https://doi.org/10.1016/j.eswa.2023.119559

[17] Chi, H., Lu, Y., Liao, B., Xu, L., & Liu, Y. (2021). An Optimized Quantitative Argumentation Debate Model for Fraud Detection in E-Commerce Transactions. *IEEE Intelligent Systems*, *36*(2), 52-63. https://doi.org/10.1109/MIS.2021.3071751

[18] Cui, Y., Han, X., Chen, J., Zhang, X., Yang, J., & Zhang, X. (2025). FraudGNN-RL: A Graph Neural

Network With Reinforcement Learning for Adaptive Financial Fraud Detection. *IEEE Open Journal of the Computer Society*, *6*, 426-437. https://doi.org/10.1109/OJCS.2025.3543450

[19] Ding, Z., Zhao, X., & Huan, R. (2024). Credit Evaluation Model and Its Application in Healthcare Insurance Fraud Detection. *International Journal of Computational Intelligence and Applications*, *23*(2), 2450005. https://doi.org/10.1142/S1469026824500056

[20] Du, H., Li, D., & Wang, W. (2022). Abnormal User Detection via Multiview Graph Clustering in the Mobile e-Commerce Network. *Wireless Communications and Mobile Computing*, *2022*, 3766810. https://doi.org/10.1155/2022/3766810

[21] Du, M. (2021). Corporate governance: five-factor theory-based financial fraud identification. *Journal of Chinese Governance*, *6*(1), 1-19. https://doi.org/10.1080/23812346.2020.1803036

[22] Fan, J., Liu, Z., Wu, H., Wu, J., Si, Z., Peng, P., & Luan, T. H. (2023). LUAD: A lightweight unsupervised anomaly detection scheme for multivariate time series data. *Neurocomputing*, *557*, 126644. https://doi.org/10.1016/j.neucom.2023.126644

[23] Guo, D. (2024). Identification and prevention of financial securities fraud based on deep learning. *Journal of Computational Methods in Sciences and Engineering*, *24*(4-5), 2673-2688. https://doi.org/10.3233/JCM-247497

[24] Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203

[25] Han, L., Wang, L., Cheng, Z., Wang, B., Yang, G., Cheng, D., & Lin, X. (2025). Mitigating the Tail Effect in Fraud Detection by Community Enhanced Multi-Relation Graph Neural Networks. *IEEE Transactions on Knowledge and Data Engineering*, *37*(4), 2029-2041. https://doi.org/10.1109/TKDE.2025.3530467

[26] He, D. (2025). A Multimodal Deep Neural Network-Based Financial Fraud Detection Model Via Collaborative Awareness of Semantic Analysis and Behavioral Modeling. *Journal of Circuits, Systems and Computers*, *34*(2), 2550054. https://doi.org/10.1142/S0218126625500549

[27] He, H., & Fang, J. (2024). Does the integration between litigation and supervision discipline financial misstatement? *China Journal of Accounting Research*, *17*(2), 100357. https://doi.org/10.1016/j.cjar.2024.100357

[28] Hu, J., Wang, S., Duan, J., Jin, H., Liu, X., & Zhu, E. (2025). Higher-order Enhanced Contrastive-based Graph Anomaly Detection Without Graph Augmentation. *Pattern Recognition*, *167*, 111666. https://doi.org/10.1016/j.patcog.2025.111666

[29] Hu, J., Zhang, Y., & Zhang, H. (2025). Hybrid optimization and deep learning for enhancing accuracy in fraud detection using big data techniques. *Peer-to-Peer Networking and Applications*, *18*(4), 179. https://doi.org/10.1007/s12083-025-01971-4

[30] Jiang, H., Peng, C., & Ren, D. (2024). Supply-chain finance digitalization and corporate financial fraud: Evidence from China. *Economic Modelling*, *139*, 106837. https://doi.org/10.1016/j.econmod.2024.106837

[31] Jiang, S., Dong, R., Wang, J., & Xia, M. (2023). Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network. *Systems*, *11*(6), 305. https://doi.org/10.3390/systems11060305

[32] Jiang, Y., & Zhao, Y. (2020). Financial fraud contagion through board interlocks: the contingency of status. *Management Decision*, *58*(2), 280-294. https://doi.org/10.1108/MD-12-2018-1355

[33] Jin, J., & Zhang, Y. (2025). The analysis of fraud detection in financial market under machine learning. *Scientific Reports*, *15*(1), 29959. https://doi.org/10.1038/s41598-025-15783-2

[34] Jin, Y. (2025). Study on digital financial fraud risk identification based on heterogeneous graph convolutional attention network. *International Journal of Networking and Virtual Organisations*, *32*(1-4), 203-218. https://doi.org/10.1504/IJNVO.2025.145376

[35] Anas K M , Rizvi S , Arora D ,et al.Decentralized Identity Management Using Self-Sovereign Identity Approach Through Blockchain[C]//International Conference on Inventive Communication and Computational Technologies.Springer, Singapore, 2024. https://doi.org/10.1007/978-981-97-7710-5_5

[36] Kong, Y., Li, Z., & Jiang, C. (2024). ASIA: A Federated Boosting Tree Model Against Sequence Inference Attacks in Financial Networks. *IEEE Transactions on Information Forensics and Security*, *19*, 6991-7004. https://doi.org/10.1109/TIFS.2024.3428412

[37] Lan, T., & Rao, Y. (2025). Financial fraud in Chinese accounting firms explained by fraud hexagon theory. *Multidisciplinary Science Journal*, *7*(12), e2025579. https://doi.org/10.31893/multiscience.2025579

[38] Lei, T., Ou, M., Gong, C., Li, J., & Yang, K. (2024). An unsupervised deep global–local views model for anomaly detection in attributed networks. *Knowledge-Based Systems*, *300*, 112185. https://doi.org/10.1016/j.knosys.2024.112185

[39] Li, C., Ding, N., Zhai, Y., & Dong, H. (2021). Comparative study on credit card fraud detection based on different support vector machines. *Intelligent Data Analysis*, *25*(1), 105-119. https://doi.org/10.3233/IDA-195011

[40] Li, E., Ouyang, J., Xiang, S., Qin, L., & Chen, L. (2025). Efficient relation-aware heterogeneous graph neural network for fraud detection. *World Wide Web*, *28*(5), 55. https://doi.org/10.1007/s11280-025-01369-5

[41] Li, F., & Duan, H. (2024). Research on Fraud Detection Method of Financial Data of Listed Companies Based on HMCRAN. *International Journal of Data Warehousing and Mining*, *20*(1). https://doi.org/10.4018/IJDWM.356510

[42] Li, H., & Yu, X. (2025). Construction of financial fraud identification model based on stacking and accounting indicators. *Journal of Computational Methods in Sciences and Engineering*, *25*(4), 3369-3383. https://doi.org/10.1177/14727978251316402

[43] Li, J. (2022). E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining. *Computational Intelligence and Neuroscience*, *2022*, 8783783. https://doi.org/10.1155/2022/8783783

[44] Li, J., Chang, Y., Wang, Y., & Zhu, X. (2023). Tracking down financial statement fraud by analyzing the supplier-customer relationship network. *Computers and Industrial Engineering*, *178*, 109118. https://doi.org/10.1016/j.cie.2023.109118

[45] Li, J., Guo, C., Lv, S., Xie, Q., & Zheng, X. (2024). Financial fraud detection for Chinese listed firms: Does managers' abnormal tone matter? *Emerging Markets Review*, *62*, 101170. https://doi.org/10.1016/j.ememar.2024.101170

[46] Li, J., & Yang, D. (2023). Research on Financial Fraud Detection Models Integrating Multiple Relational Graphs. *Systems*, *11*(11), 539. https://doi.org/10.3390/systems11110539

[47] Li, T., Kou, G., Peng, Y., & Yu, P. S. (2022). An Integrated Cluster Detection, Optimization, and Interpretation Approach for Financial Data. *IEEE Transactions on Cybernetics*, *52*(12), 13848-13861. https://doi.org/10.1109/TCYB.2021.3109066

[48] Li, W., Liu, X., & Zhou, S. (2024). Deep learning model based research on anomaly detection and financial fraud identification in corporate financial reporting statements. *Journal of Combinatorial Mathematics and Combinatorial Computing*, *123*, 343-355. https://doi.org/10.61091/jcmcc123-24

[49] Li, X., Kim, J. B., Wu, H., & Yu, Y. (2021). Corporate Social Responsibility and Financial Fraud:

The Moderating Effects of Governance and Religiosity. *Journal of Business Ethics*, *170*(3), 557-576. https://doi.org/10.1007/s10551-019-04378-3

[50] Liao, B., Huang, Z., Cao, X., & Li, J. (2022). Adopting Nonlinear Activated Beetle Antennae Search Algorithm for Fraud Detection of Public Trading Companies: A Computational Finance Approach. *Mathematics*, *10*(13), 2160. https://doi.org/10.3390/math10132160

[51] Liu, L., Tsai, W. T., Bhuiyan, M. Z. A., Peng, P., & Liu, M. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. *Future Generation Computer Systems*, *128*, 158-166. https://doi.org/10.1016/j.future.2021.08.023

[52] Liu, Q. X., Zhang, J. G., & Tan, B. (2024). Financial Fraud Recognition Model Based on Privacy Preserving and Federated Learning. *Journal of Network Intelligence*, *9*(4), 2360-2374. https://bit.kuas.edu.tw/~jni/2024/vol9/s4/27.JNI-S-2024-01-023.pdf

[53] Liu, Y., Wu, B., & Zhang, M. (2023). Can independent directors identify the company's risk of financial fraud. *China Journal of Accounting Studies*, *11*(3), 465-492. https://doi.org/10.1080/21697213.2023.2239670

[54] Button M .Fraud investigation and the 'flawed architecture' of counter fraud entities in the United Kingdom[J].International Journal of Law Crime & Justice, 2011, 39(4):249-265. https://doi.org/10.1016/j.ijlcj.2011.06.001

[55] Lu, P., Wang, Y., & Li, B. (2024). Short selling and corporate financial fraud: Empirical evidence from China. *International Review of Economics and Finance*, *89*, 1569-1582. https://doi.org/10.1016/j.iref.2023.09.011

[56] Lu, W., & Zhao, X. (2020). Research and improvement of fraud identification model of Chinese A-share listed companies based on M-score. *Journal of Financial Crime*, *28*(2), 566-579. https://doi.org/10.1108/JFC-12-2019-0164

[57] Lu, Y., Hao, J., & Tang, X. (2025). Dual-model synergy for audit opinion prediction: A collaborative LLM agent framework approach. *International Review of Economics and Finance*, *104*. https://doi.org/10.1016/j.iref.2025.104642

[58] Ma, J., Xiang, S., Li, Q., Yuan, L., Cheng, D., & Jiang, C. (2025). Parallel Graph Learning With Temporal Stamp Encoding for Fraudulent Transactions Detections. *IEEE Transactions on Big Data*, *11*(4), 1945-1958. https://doi.org/10.1109/TBDATA.2024.3499338

[59] Miao, Z. (2024). Financial Fraud Detection and Prevention: Automated Approach Based on Deep Learning. *Journal of Organizational and End User Computing*. https://doi.org/10.4018/JOEUC.354411

[60] Ming, R., Mohamad, O., Innab, N., & Hanafy, M. (2024). Bagging Vs. Boosting in Ensemble Machine Learning? An Integrated Application to Fraud Risk Analysis in the Insurance Sector. *Applied Artificial Intelligence*, *38*(1). https://doi.org/10.1080/08839514.2024.2355024

[61] Murad, M., Othman, S., & Kamarudin, M. A. I. (2025). Entrepreneurial university input, core strategic plan and output. *Entrepreneurship Education*, *8*(1), 99-129. https://doi.org/10.1007/s41959-025-00137-w

[62] Peng, Z., Yang, Y., & Wu, R. (2022). The Luckin Coffee scandal and short selling attacks. *Journal of Behavioral and Experimental Finance*, *34*. https://doi.org/10.1016/j.jbef.2022.100629

[63] Qiu, S., & Luo, Y. (2024). How to detect and forecast corporate fraud by media reports? *Journal of Forecasting*, *43*(1), 58-80. https://doi.org/10.1002/for.3022

[64] Raza, M. W., & Ye, J. (2025). Beyond Sharpe ratio: comparison of risk-adjusted performance of Shariah-compliant and conventional indices. *International Journal of Islamic and Middle Eastern Finance and Management*, *18*(1), 184-200. https://doi.org/10.1108/IMEFM-01-2024-0013

[65] Rind, A. A., Sarang, A. A. A., Kumar, A., & Shahbaz, M. (2023). Does financial fraud affect implied cost of equity? *International Journal of Finance and Economics*, *28*(4), 4139-4155. https://doi.org/10.1002/ijfe.2639

[66] Shao, M., Lin, Y., Peng, Q., Zhao, J., Pei, Z., & Sun, Y. (2023). Learning graph deep autoencoder for anomaly detection in multi-attributed networks. *Knowledge-Based Systems*, *260*. https://doi.org/110084

[67] Shou, M., Bao, X., & Yu, J. (2023). An optimal weighted machine learning model for detecting financial fraud. *Applied Economics Letters*, *30*(4), 410-415. https://doi.org/10.1080/13504851.2021.1989367

[68] Shuai, S., Hu, Z., Zhang, B., Liaqat, H. B., & Kong, X. (2023). Decentralized Federated Learning-Enabled Relation Aggregation for Anomaly Detection. *Information*, *14*(12). https://doi.org/10.3390/info14120647

[69] Steven, P. H. (2025). Reinforcing Financial Growth in Metaverse Organizations. *Journal of Metaverse Business Designs*, *6*(1), 1-11. https://doi.org/10.70890/JMBD.2025.6101

[70] Sun, Q., Tang, T., Chai, H., Wu, J., & Chen, Y. (2021). Boosting fraud detection in mobile payment with prior knowledge. *Applied Sciences*, *11*(10). https://doi.org/10.3390/app11104347

[71] Sun, Y., Zeng, X., Xu, Y., Yue, H., & Yu, X. (2024). An intelligent detecting model for financial frauds in Chinese A-share market. *Economics and Politics*, *36*(2), 1110-1136. https://doi.org/10.1111/ecpo.12283