NFSU JOURNAL OF FORENSIC ACCOUNTING & FRAUD INVESTIGATION

VOLUME 2 • ISSUE 1 • JANUARY–JUNE 2026
E-ISSN: 3107-4650
njfafi.nfsu.ac.in

Article ID: J-2026-0032

Beyond the Fraud Triangle: Integration of Fraud Pentagon and Hexagon Models in Digital Environments

Dhara Mehta[1*]

Assistant Professor, SEMCOM, Charutar Vidya Mandal (CVM) University, Vallabh Vidyanagar, Anand, Gujarat, India

*Corresponding author e-mail: dharamehta174@gmail.com

***Abstract*—Traditional fraud detection methods such as the Fraud Triangle have found it challenging to adapt to the growing complexity of financial fraud occurring in online environments. More comprehensive frameworks such as the Fraud Pentagon and Fraud Hexagon, which add further organisational and behavioural elements help provide insight into the theoretical knowledge base surrounding fraud. However, they do not sufficiently incorporate operational technology and the digital environment that characterises today's forms of fraud. This study proposes a unified conceptual framework to digital ecosystems by integrating the Fraud Triangle, Fraud Pentagon, and Fraud Hexagon into one coherent model. By adding components such as digital anonymity, technology support, and cyber behavioural incentive, the proposed Digital Fraud Integrated Model (DFIM) provides a more thorough understanding of fraud in the environments of the current day and beyond. The research provides contributions to the theory of forensic accounting and offers insight for auditors, regulators, and organisations making the transition into artificial intelligence and technology-enabled financial environments.**

***Index Terms*—Fraud Triangle, Fraud Pentagon, Fraud Hexagon, Digital Fraud, Forensic Accounting.**

I. Introduction

The recent technological advances in the digital world, the proliferation of Financial Technology companies (Fintechs) and the entry of Artificial Intelligence in business processes are all factors that have drastically changed how we do business in the world today, particularly in the financial services sector, over the last two decades. Fintech, digital technologies and AI have all added to the efficiencies, accessibility and creativity of the financial services business. However, with these advances come additional opportunities for Fraud. Historically, Fraud was the result of internal collaboration and the manual alteration of financial records; however, it has evolved from that type of activity to a sophisticated, technologically-enabled issue that extends beyond national and organisational boundaries [1].

In this dynamic, ever-evolving environment, fraud is becoming increasingly sophisticated, mobile, and difficult to detect. Typical internet crimes like phishing, identity theft, crypto currency fraud, and electronic payment fraud have drastically risen in instances, particularly in countries with developing digital economies. Many of these criminal activities use modern technologies to outwit traditional controls. In particular, the use of AI and automated systems in business operations has made the process of detecting fraud much more difficult. As businesses continue to transition to digital platforms and work remotely, the reliance on virtual communications continues to grow, while the amount of physical supervision has decreased, creating increased opportunities for fraudulent activity [1].

Despite these developments in the arena of law enforcement and criminal justice, traditional models such as the Fraud Triangle remain among the most significant theoretical foundations of fraud detection as it pertains to forensic accounting. The Fraud Triangle, created by Cressey in 1953, comprises three elements that lead to fraud: opportunity, pressure (or motivation), and rationalization. This framework has become a cornerstone for many forensic investigations and auditing standards because of its straightforwardness and inherent appeal. Critics maintain that the Fraud Triangle does not account for many of the complexities related to contemporary organizational and technological systems, providing an unnecessarily simplistic understanding of human behavior [2].

The Fraud Triangle has received criticism for its oversimplified assumptions about fraud and its inability to explain the complex nature of fraud behaviour seen today. Researchers believe that fraud is a result of multiple different psychological characteristics, organisational dynamics and systemic influences, and that fraud cannot be completely explained by looking at just situational factors alone. Because of these limitations, scholars have begun modifying traditional models to provide a more realistic depiction of the type of modern fraud seen today [3].

The Fraud Pentagon was designed to augment the traditional Fraud Triangle by incorporating two additional factors: capability and arrogance. Arrogance pertains to an individual's feeling of superiority or excessive confidence that causes them to disregard internal control and ethical

limitations, and capability indicates a person's access, skills, and aptitude for committing fraud or taking advantage of their organization's internal processes. Thus, this model demonstrates that both personal attributes and types of behaviour that enable or continue fraud are equally as influential in producing fraudulent conduct as the situational forces at play [4].

[5] In regard to fraud, the Fraud Hexagon model uses an expansion of this theory and adds one more element to the definition of the model; collusion. Many of today's most common forms of fraudulent activity involve agents working together in some manner. As fraud has become more complicated and required cooperation between agents in order to complete the fraud solution, collaborating as part of the operation has moved fraud investigation away from individual-focused fraud theories and into collaborative (network) type fraud explanations [6].

Even though these alternative fraud models provide some valuable academic perspective, they remain predominantly focused on behaviour, and do not take sufficient account of the technological elements now fundamental to emergent digital fraud. Traditional models, such as the Fraud Triangle and its derivatives, put their emphasis on organisational and psychological variables, and virtually ignore the manner in which technological tools and digital infrastructures enable fraudulent behaviour [7]. The rapid proliferation of digital platforms, artificial intelligence (AI) and Fintech ecosystems has given rise to different types of fraud risk, including identity-based fraud, automated cyber-attacks, and system manipulation, which increase the complexity of financial crimes [1]. Furthermore, the widespread adoption of generative AI technologies, such as deep fakes and synthetic identities, also enormously increases the complexity of fraud schemes making it more difficult to detect them and requiring the application of increasingly sophisticated analytical methodologies [8].

Fraud in the digital world is highly influenced by anonymity. The "online disinhibition effect" describes how people behave with less self-control and act more impulsively while in an anonymous environment on the Internet. Because of this online disinhibition effect, there is a decreased sense of accountability for one's actions and therefore, increased chances that people will act unethically or commit fraudulent acts due to their perception that they are anonymous and not connected to any real-world consequences [9].

Fraud risk to organizations has increased in the post-COVID-19 world because of the migration to remote work and the digital economy. Many reasons contribute to this increased risk including decreased supervision due to the remote workforce, increased reliance on a variety of digital platforms and tools, and increased financial and psychological pressures. This environment creates a situation in which fraud is much easier to justify and misconduct can more readily occur. In addition, fraud perpetrators are able to create very sophisticated fraud schemes using artificial intelligence technology; for example, they use deep fake videos and automatically generated fraud scripts to commit fraud [10].

Given these recent events, we must now revisit and expand our understanding of fraud theories to include both digital and technological components. Although the Fraud Triangle, Fraud Pentagon, and Fraud Hexagon models of fraud give a foundation for understanding how fraudsters act, they are not designed to account for the interplay between human actions and technology. Therefore, a unified theoretical framework for explaining digital ecosystems in relation to fraud is necessary [11].

This research provides a comprehensive concept framework of Digital Fraud Integrated Model (DFIM) which takes an overall view of how traditional and extended fraud theory constructions work with technology, technology facilitation, and digital anonymity to describe fraud types such as criminal behaviour; employee behaviour; cyber, e-commerce and invoices; and other related behaviours. The DFIM model provides an all-inclusive framework for understanding fraud-related behaviours in the digital world by considering three different perspectives: Behavioural, Organisational, and Technological [12].

This research adds to the body of literature in several ways. First, it helps to create fraud theory by bridging the gap between traditional behavioural models of fraud and the new wave of digital fraud. Second, it offers practical implications not only for auditors and forensic accountants but also for regulators in that it has defined the digital risk factors relevant to fraud detection and prevention strategies. Finally, the proposed model is a basis for future empirical research that utilises advanced analytic techniques, such as Structural Equation Modelling (SEM) and Partial Least Squares (PLS), creating relevance across various organisational and geographical jurisdictions [13].

II. Literature Review

A. Evolution of Fraud Theories

Fraud has long been a prominent topic in the literature regarding accounting and auditing because of the substantial negative economic and reputational consequences of committing fraud. The Fraud Triangle [2], represents the underlying theory behind the occurrence of fraud – it identifies three elements that contribute to perpetrating fraud: (1) pressure; (2) opportunity; and (3) rationalisation. While this is a useful tool and helpful in understanding fraud, critics have pointed out that the model fails to fully explain the complexity of fraud within contemporary organisational settings. Additionally, research has found that factors other than individual motivation influence the commission of fraud; namely, both organisational and environmental factors influence the behaviour of individuals in regards to committing fraud [14].

The limitation of existing frameworks led researchers to create expansive frameworks, such as Fraud Diamond (which includes capability), Fraud Pentagon (which adds arrogance), and Fraud Hexagon (which adds collusion). These new types of frameworks demonstrate the growing

acknowledgment among those studying fraud that fraud has many dimensions and cannot simply be understood with uncomplicated models [7].

B. Fraud Pentagon Model

Capability refers to an individual's ability, expertise and position, enabling them to effectively commit fraud, while Arrogance represents a dominant manager that is overconfident about their capability to violate policies or regulations they believe don't apply to them; or, to put it another way, they consider themselves above internal controls [15].

The empirical research shows that those with a high level of authority, confidence , and disregard for internal control will often engage in override of controls leading to fraud. But there is additional evidence suggesting that these behavioral factors alone are insufficient to fully account for fraud occurring within more complicated environments — Specifically where complex technological system infrastructure plays a significant role [16].

C. Fraud Hexagon Model

The Fraud Hexagon adds another level of explanation by adding an additional component of collusion. Since most fraud within modern organizations is performed by colluding between multiple individuals, this recognizes that organizations will typically commit fraud through co-ordinated efforts rather than with the actions of only one individual. Collusion can be seen as particularly applicable to cases where there are several individuals working together to commit large-scale corporate frauds or cyber-based frauds by taking advantage of weaknesses within their systems. Research shows that collusion can greatly increase the difficulty in detection, increase the complexity of the fraud and increase the potential for large losses arising from the fraud [17].

In summary, while the Pentagon and Hexagon fraud models have evolved to include the added component of collusion, both models remain primarily focussed on behavioural and organisational issues and do not specifically consider digital and technological factors that may impact fraud.

D. Digital Transformation and Fraud Risk

[18] Fraud is drastically different now than before due to the rapid digitalisation of our financial services and new technologies such as artificial intelligence (AI), big data analytics, and cloud computing. Technology has completely changed how fraud is committed and detected. Digital environments have also created many new risks associated with fraud including:

- Cyber fraud/identity theft
- Automated fraud using AI
- International digital transactions
- Manipulating digital records

The techniques used today to detect traditional fraud are not sufficient to identify today's advanced forms of fraud anymore. There are many tools that help to find irregularities and better identify fraud in real-time through the use of AI-based systems [19].

E. Organizational and Governance Factors

Fraud acts are still a prevalent problem today. Many organizational factors contribute to the occurrence of fraud. If your company has weak internal controls, ineffective governance structures, or poor monitoring mechanisms, you are at increased risk for fraud. Research results from studies using PLS-SEM methods definitively indicate that the effectiveness of internal control elements such as risk assessment, communication, and monitoring will influence fraud prevention effectiveness [20].

The combination of an organization's technological capabilities and internal controls can significantly improve fraud detection effectiveness and audit quality through the implementation of artificial intelligence ("AI") in the fraud detection process and business analytics [9].

F. Research Gap

Even though theories about the development of Fraud have evolved, there are still some key gaps that exist:

- Over-reliance on individual behavioural elements
- Fairly limited consideration of the dynamics of groups/large numbers of players that might collude
- Not enough integration of the various digital technologies and/or variables
- No suitable mechanisms to effectively analyse fraud within a complex digital environment.

III. Methodology

A. Research Design

The qualitative–quantitative secondary data-based research design used in this study combines a systematic literature review (SLR) and conceptual/theoretical synthesis to analyse how fraud theories have evolved and been integrated into digital environments. The research is exploratory and explanatory in nature, with the following objectives:

- To explore the inadequacies of traditional fraud models
- To evaluate the extensions of fraud models, such as the Fraud Pentagon and Fraud Hexagon
- To assess the impact of digital transformation on fraud dynamics
- To identify an integrated theoretical framework

B. Research Approach

This research employs a deductive methodological approach to assess and build upon current theories such as the Fraud Triangle, Fraud Pentagon, and Fraud Hexagon. It uses elements of conceptual synthesis and inductive reasoning to create new digital fraud constructs including technology facilitation, digital anonymity, and system complexity.

C. Data Collection

Only secondary data will be used in this project; the data will include peer-reviewed articles from academic journals,

conference articles, academic reports and books published by reputable sources. Peer reviewed references were collected from a variety of different databases, such as Google Scholar, PubMed, and Science Direct.

To ensure the quality and relevance of the data used for this project, very specific inclusion and exclusion criteria had to be met when selecting literature for inclusion in this project.

Inclusion Criteria:

- Articles published from 2010-2026
- Academic research that pertains to the use of fraud theories (the Fraud Triangle, the Fraud Pentagon, and the Fraud Hexagon) as a means of evaluating and/or detecting fraud
- Studies that relate to digital fraud, cyber fraud, AI-based fraud detection or technology-based fraud risk
- Articles published in peer-reviewed journals, reputable academic journals or through academic publishers

Exclusion Criteria:

- Articles published in non-peer-reviewed or unreliable academic journals
- Studies that would not fit within the realm of fraud theories or the digital environment as a whole
- Studies that are at least a quarter century or older, re-published, and/or do not add substantially to existing research on the related topic.

D. Systematic Literature Review (SLR) Process

The study employs a Systematic Literature Review (SLR) strategy that will help to provide a systematic and transparent examination of prior research to best inform the current study. There are four stages in this systematic process:

First, at the identification stage, an extensive amount of relevant literature was gathered using various keywords (Fraud Triangle, Fraud Pentagon, Fraud Hexagon, Digital Fraud, Cyber Fraud and AI Based Fraud Detection) from leading research-based databases.

Second, at the screening stage, duplicates and irrelevant studies were removed based on their titles and abstracts.

Third, at the eligibility stage, full text articles were reviewed to determine if they met the required selection criteria: relevance to the research question, theoretical contribution, and alignments with the research objectives.

Fourth, at the inclusion stage all studies that were of high quality and/or relevance to the research objectives that had met all of the previous selection criteria were retained for further analysis.

Using this systematic methodological process will ensure that the study's results are based on credible, comprehensive and specifically relevant literature which improves the reliability of the theoretical findings conceptualised in this study.

E. Limitations of the study

- Dependence on existing literature
- Lack of primary empirical validation
- Possibility of publication bias

IV. Conceptual Findings and Analysis

A. Conceptual Findings Overview

This investigation employs a conceptual framework that relies on secondary data to access the nature of fraud and thus the findings do not come from primary statistical analysis, but as a result of the researchers synthesizing existing empirical and theoretical literature. By synthesizing existing body of empirical work on contemporary fraud, and significant fraud theories such as Fraud Triangle, Fraud Pentagon and Fraud Hexagon; this dissertation has created a comprehensive understanding of fraudulent behaviour in today's organisations [21].

According to the conceptual synthesis it is evident that existing behavioural frameworks are no longer adequate at accounting for fraud. Fraud should be perceived as an ever-evolving and complex phenomenon, which results from the combination of technological infrastructures, organisation control systems, collaborative networks, and individual behavioural motivation. The rise of digital platforms, big data analytics, and artificial intelligence (AI) over the last few years has established new dynamics in relation to fraud and created both very sophisticated means for committing fraud and the development of state-of-the-art detection techniques for identifying fraud [22].

B. Behavioural Drivers: Core but Insufficient

The findings suggest that behaviours are a fundamental foundation of fraud theory and are a key influence in deciding if someone will commit fraud as described by the Fraud Pentagon Theory, which identifies four core factors (pressure, rationalization, capability, and arrogance) determining whether an individual has a propensity to commit fraud. The primary driving force in an individual's decision to commit fraud is usually due to some type of financial, organizational, or personal pressure. The notion of capability identifies the level of technical skill to commit the fraud or the authority to commit the fraud. Moreover, the rationalization component allows individuals to justify committing fraud, whereas the arrogance component provides an individual with the belief that they will not suffer any consequences by violating authority figures.

Empirical evidence exists in support of the behavioural constructs of fraud being an essential explanation for the occurrence of fraud within organizations and especially among individuals employed at the managerial level [23].

However, the conceptual study refers to the many limitations of behavior-centered models of fraud. These models fail to adequately account for systemic, organizational, and technological influences when considering fraud, as they are focused solely on the individual decision-making process and therefore cannot address the complexity, scale, and digitally enabled transactions associated with fraudulent activities. Therefore, it is necessary to incorporate behaviour with additional structural and technological factors that are both necessary and not sufficient to adequately explain the fraud phenomenon.

C. Organizational Factors and Dynamic Opportunity

The research indicates that the concept of opportunity has shifted considerably in modern work settings. In the past, opportunity was associated solely with inadequate internal controls, whereas presently, opportunity is viewed as a dynamic concept that is influenced by the quality of governance, the transparency of systems and networks, and the digital technologies used to create them.

Internal control systems that operate effectively are vital to reducing fraud risk, particularly those that employ effective risk management strategies for monitoring and communication. The available empirical evidence [24] suggests that employing effective internal controls reduces the likelihood of fraud occurring because such controls improve both the chances of detecting fraud and holding those committing fraud accountable.

Deficiencies in auditing frameworks, communication channels, and the structure of governance contribute to systemic vulnerabilities. These vulnerabilities facilitate immoral behaviour by increasing information asymmetries and promoting the potential for fraud. In addition, the effects of deficiencies in these areas are more pronounced in digital environments, which make opportunity a dynamically evolving risk factor.

D. Collusion and Network-Based Fraud

The introduction of the idea of collusion as a function of the Fraud Hexagon model is an important conceptual advance of this work. Modern fraud is increasingly being defined by the coordinated actions of multiple individuals or groups rather than just independent actions.

Collusion enhances the potential of fraud by providing individuals with the means to share information, work together to create fraudulent systems and conceal their fraud. Studies show that cooperative fraud reduces the chance of detection and makes the fraud significantly more complex [23].

Most importantly, this research identifies collusion as a multiplicative factor. Through the circumvention of internal controls, collusion creates additional opportunities for fraud, reduces detection through the coordinated concealment of fraud and increases the potential consequences of capacity. This supports the concept of fraud being treated as a systems problem created by the network effects of organizations.

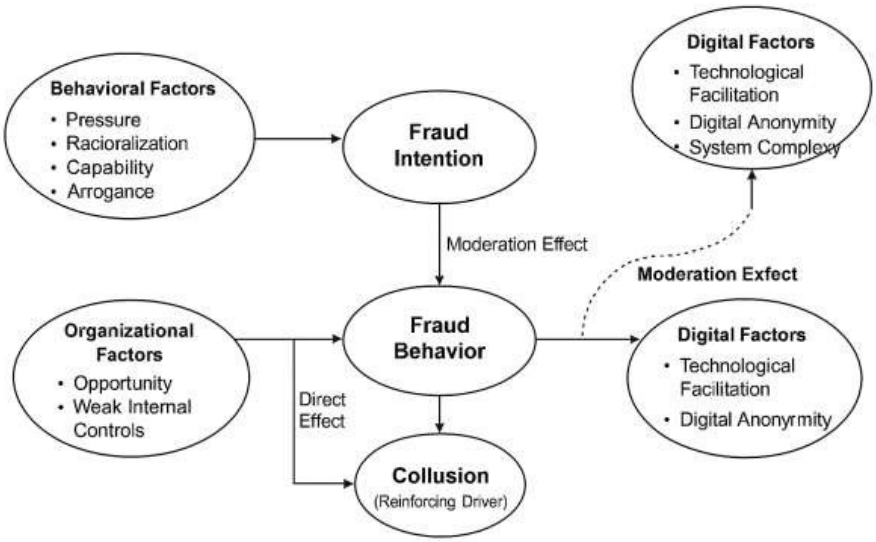


Fig. 1.

E. Digital Fraud Integrated Model (DFIM)

Fraud is a universal phenomenon viewed through four components - organizational, network, and technology and behavioural. How often and where fraud occurs depends both on organisational factors (opportunity, governance, internal controls) and behavioural factors (pressure, rationalisation, ability, hubris). Collusion is a second part of the model and relates to the increase in the number of people who can participate in fraud through networks as well as organisational structures that make it easier for people to commit fraud.

Second, in a digital environment, the technology or ways of facilitating fraud by using digital technologies, such as using anonymity online or using artificial intelligence or the increasing technical complexity of systems will impact and greatly enhance the ability for people to commit fraud.

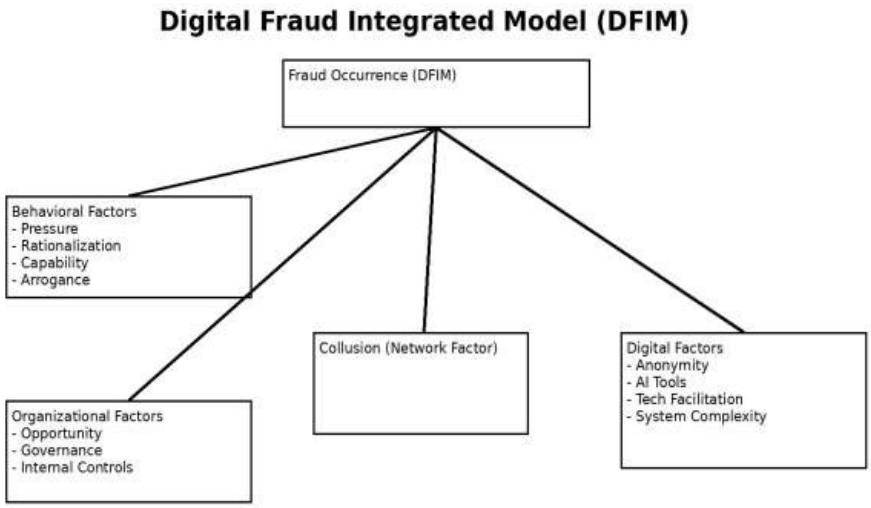


Fig. 2.

F. Development of Hypotheses

The hypotheses proposed in this research artia are based on the Digital Fraud Integrated Model. Each theoretical hypothesis combines elements from the four categories discussed above: individual behaviour; organisation; network; and technology.

1) Behavioral Factors and Fraud Occurrence: Behavioral factors play an important role in understanding fraud. They have their origins in the original Fraud Triangle Concept and the newly expanded Fraud Pentagon Concept, which further defined behavioral factors. While rationalization allows a person to justifiably rationalize their own unethical behavior, pressure provides an incentive to commit fraud/lying. Arrogance represents the belief of a person to be able to circumvent internal controls and not be held accountable for his/her actions. Capability provides the specific knowledge and skillset a person needs to perpetrate fraud.

Since there is less oversight within the digital environment and therefore a greater reliance on virtual systems, these behavioral traits are amplified.

H1: Behavioral factors (pressure, rationalization, capability, and arrogance) will have a positive and significant correlation to the amount of fraud being committed.

2) Organizational Factors and Fraud Opportunity: Fraud opportunities are greatly influenced by the organization's internal controls, governance procedures and monitoring systems. Weak governance structures and poor control systems create vulnerabilities that can be exploited and increase the risk of fraud. However, strong internal control systems reduce the risk of fraud.

The concept of opportunity also becomes more fluid in the digital realm due to the complexity of technology and system vulnerabilities.

H2: Organizational factors (opportunity, governance quality and internal control) have a strong relationship with the occurrence of fraud, in digital environments.

3) Collusion and Network-Based Fraud: Fraud continues to be a problem in today's society, and the Fraud Hexagon model shows that collusive behavior is a significant contributor to this issue. In digital environments, fraud is often committed by multiple parties to perpetrate the fraud, either as individuals or organizations, working in combination. Collusion enables the success of fraud schemes by distributing duties, concealing activity, and reducing the chance of detection.

H3: The occurrence of fraud in digital environments has a positive and significant relationship with collusion.

4) Digital Factors and Fraud Occurrence: The digital aspects of the DFIM, such as digital anonymity, technological facilitation, AI tools, and system complexity, are among its biggest achievements. These attributes have the ability to change the dynamics of fraud by reducing responsibility... enhancing performance efficiency during action..., and allowing large-scale frauds to take.

H4: Digital elements (digital anonymity, technological facilitation, AI tools and system complexity) are positively correlated to occurrence of fraudulent activity.

5) Moderating Role of Digital Factors: Digital environments not only have a direct impact on fraud, but also reshape how traditional fraud triggers operate. Digital technology can enhance capability and create additional opportunities for fraud, while anonymity provided by digital means can enhance the rationalization of fraud.

H5: Digital elements act as moderating variables in the relationships between behavioral motivators and incidence of fraud such that digital environments strengthen those relationships.

6) Integrated Effect of DFIM Components: Fraud, based upon the DFIM paradigm, is a multi-faceted concept and may be influenced by an aggregate of different elements such as: Behaviour; Organization; Collusion; Digital. H6: There is a significant combined influence of Behavioural, Organizational, Collusive, and Digital elements on Fraud occurrence within Digital Environment.

V. Conclusion

This research was conducted using a secondary data-analytical design that conceptualizes the application of the Fraud Pentagon and Fraud Hexagon models concerning digital contexts, thereby expanding upon existing fraud theory literature. Through systematic analysis, the results of the investigation provide a comprehensive understanding of how fraudulent behaviour has evolved as a result of increased complexity in organisations, collaborative mechanisms and advances in technology.

The findings indicate that although earlier models (e.g., Fraud Triangle and its variations) continue to serve as theoretically sound tools, they are insufficient—on their own—to adequately account for the complexities of modern-day fraud. The same behavioural variables (e.g., pressure, rationalisation, capability and arrogance) remain the primary causes of fraudulent intent. However, when combined with organisational and environmental variables, their utility increases exponentially. Opportunity, for example, is no longer viewed as a fixed point; instead, it is characterised as being fluid and influenced by the quality of digital infrastructure, internal controls and governance.

The Fraud Hexagon model identifies that collusion plays an important part in fraud, which is a core contribution of the study. These results suggest that fraud is increasingly becoming a collaborative character, and that there are multiple people cooperating together to commit fraud. Adding capabilities, increasing opportunity, and reducing the likelihood of detection through collusive methods increases the risks associated with committing fraud. Therefore, the findings indicate a need for a shift from fraud theories focused on individuals to fraud theories based on their relationships and systemic characteristics.

Additionally, the current study identifies that modern fraud behavior is predicted by digital characteristics. Complexity of systems, anonymity in digital environments, and convenience of technology have a substantial influence on the detection and occurrence of fraud. Technological advancement is enhancing detection systems via AI-based analytics/products, as well as providing new ways to commit fraud. Hence, technology does not merely act as a contextual element but rather plays an active role within the overall fraud ecosystem.

Overall, this analysis reveals that businesses, auditors and regulators need access to and use of new technology based fraud prevention techniques, strengthen internal controls with internal systems and enhance digital skills. The increasing sophistication of fraud requires a proactive, collaborative approach that combines the latest technological solutions with behavioral intelligence.

The limitations of this study are associated with relying on conceptual analysis and secondary data; therefore, to build upon the theoretical framework of this research, empirical investigations using Structural Equation Modelling (SEM) or PLS-SEM methods within different industries and geographic locations should be conducted.

References

[1] T. Khiaonarong and S. Zheng, "The Rise of Cyber Events and Digital Fraud in the Financial Sector," *IMF Working Papers*, International Monetary Fund, pp. 1–33, 2026.

[2] D. Cressey, "Fraud Triangle: Elements, Prevention, and Legal Risk," 1953.

[3] P. Tickner and M. Button, "Deconstructing the Origins of Cressey's Fraud Triangle," *Journal of Financial Crime*, vol. 28, no. 3, pp. 1–12, 2021, doi: 10.1108/jfc-10-2020-0204.

[4] T. Achmad, D. I. Hapsari, and I. D. Pamungkas, "Analysis of Fraud Pentagon Theory to Detecting Fraudulent Financial Reporting using F-Score Model in State-Owned Companies Indonesia," *WSEAS Transactions on Business and Economics*, pp. 124–133, 2022.

[5] M. Elbagoury, "The Fraud Hexagon: A New Lens on Why Fraud Happens," 2025.

[6] H. M. Ghaisani, Triyono, and A. B. Bawono, "Analysis of Financial Statement Fraud: The Vousinas Fraud Hexagon Model Approach and the Audit Committeas Moderating Variable," *The International Journal of Business Management and Technology*, pp. 115–125, 2022.

[7] G. Burlacu, I.-B. Robu, I. Anghel, M. E. Rogoz, and I. Munteanu, "The Use of the Fraud Pentagon Model in Assessing the Risk of Fraudulent Financial Reporting," *Risks*, vol. 13, no. 6, Art. no. 102, pp. 1–20, 2025, doi: 10.3390/risks13060102.

[8] L. S.F. Lin, "Examining the Role of Deepfake Technology in Organized Fraud: Legal, Security, and Governance Challenges," *Frontiers in Law*, pp. 6–17, 2025.

[9] Y. P. Siswanto, D. Dananjaya, and D. Soeindra, "Fraudulent Analysis of Financial Statements onReal Estate & Property Companies 2015-2019:Hexagon Theory Approach," *International Journal of Research and Analytical Reviews*, 2022.

[10] D. Cumming, C. Firth, J. Gathergood, and N. Stewart, "Work-from-homeandtheriskofsecurities misconduct," *Eur Financ Manag*, pp. 1–24, 2023.

[11] A. Glebovskiy, "The Fraud Triangle and Model of Criminogenesis," *International Journal of Law and Society*, pp. 115–127, 2021.

[12] T. N. Odonkor, T. T. Adewale, and T. D. Olorunyomi, "AI-Powered financial forensic systems: A conceptual framework for fraud detection and prevention," *Magna Scientia Advanced Research and Review*, pp. 120–137, 2021.

[13] K. Goyal, M. Garg, and S. M., "Adoption of artificial intelligence-based credit risk assessment and fraud detectionin the banking services: a hybrid approach," *Future Business Journal*, pp. 1–20, 2025.

[14] J. S. Yanti, Y. Diantimala, and A. Nuraini, "Testing the Crowes Pentagon Theory of Fraud on Financial Statement Fraud," *International Journal of Management, Accounting and Economics*, pp. 296–312, 2024.

[15] D. Wibowo, "Factors that Influence Financial Statement Fraud with Fraud Pentagon Analysis," *Asia Pacific Fraud Journal*, n.d.

[16] F. Tjahjani and B. M. Rizky, "FRAUD PENTAGON THEORY: INDICATION TOWARD FRAUDULENT FINANCIAL REPORTING ON NON-BANKING SECTOR," *International Journal of Economics, Business and Accounting Research (IJEBAR)*, pp. 1–12, 2022.

[17] J. D. Mvunabandi, "Scholarly Discourse of Remote Forensic Auditing and Fraud Schemes in Remote Workforce: AScoping Review," *International Journal of Applied Research in Business and Management*, pp. 1–35, 2024.

[18] A. Cahyati, "Effect of Pressure, Opportunity, Rationalizations, Capability and Arrogance in The Concept of The Fraud Pentagon," *Journal of Auditing, Finance, and Forensic Accounting*, pp. 1–11, n.d.

[19] N. Christian, Y. Z. Basri, and W. Arafah, "Analysis of Fraud Triangle, Fraud Diamond and Fraud Pentagon Theory to Detecting Corporate Fraud in Indonesia," *The International Journal of Business Management and Technology*, pp. 73–78, 2019.

[20] A. Riyanti and T. Trisanti, "The Effect of Hexagon Fraud on the Potential Fraud Financial Statements with the Audit Committee as a Moderating Variable," *International Journal of Social Science And Human Research*, pp. 2924–2933, 2021.

[21] L. T. Thuy, "A Structural Analytical Framework for Technology-Driven Fraud Detection and Audit Outcomes," *International Journal of Analysis and Applications*, pp. 1–20, 2026.

[22] C. Alorh, "Harnessing artificial intelligence for financial fraud detection through cybersecurityintegrated models ensuring real-time anomaly tracking and mitigation," *International Journal of Science and Research Archive*, pp. 1586–1603, 2024.

[23] T. Achmad, I. Ghozali, M. R. Helmina, D. I. Hapsari, and I. D. Pamungkas, "Detecting Fraudulent Financial Reporting Using the Fraud Hexagon Model: Evidence from the Banking Sector in Indonesia," *Economies*, vol. 11, no. 1, Art. no. 5, pp. 1–17, 2022, doi: 10.3390/economies11010005.

[24] A. Vutumu, O. Aregbeyen, and A. S. Akinteye, "Internal Control and Fraud Prevention in the Nigerian Public Sector: A Partial Least Square Structural Equation Modeling Approach," *Journal of Financial Risk Management*, pp. 703–729, 2024.