Journal of Management Science Research Review
https://jmsrr.com/index.php/Journal/about

Volume 5 Issue No 1 (2026)

Online ISSN: 3006-2047
Print ISSN: 3006-2039

Online Financial Fraud and the Role of Financial Technology in Mitigation

Iftikhar Ahmad
Riphah School of Leadership Malakand, Faculty of Management Sciences, Riphah International University Malakand Campus. Email: iftikhar.ahmad@riphah.edu.pk, iftikharswati@gmail.com,

Faisal Amjad
Riphah School of Leadership Malakand, Faculty of Management Sciences, Riphah International University Malakand Campus Email: faisalamjad.ms@gmail.com

Ilyas Sharif (Corresponding Author)
Quaid-e-Azam College of Commerce, Faculty of Management & Information Sciences, University of Peshawar. ilyasqacc@uop.edu.pk

Abid Khan (Corresponding Author)
University of Malakand, Email: drabidkhan21@gmail.com

Abstract
This study examines the potential of FinTech innovations to minimize online financial fraud through an integrated model of behavioural biometrics and decentralized self-sovereign identity (SSI) systems. The evaluation examines cyber fraud tactics that exploit weaknesses in traditional authentication while assessing whether behavioral authentication and decentralized identification mechanisms can enhance digital trust without compromising usability. A mixed-method research approach was employed in this study while the data of 100 financial services firms was collected through a structured survey. These organisations encompass banks, FinTech companies, and payment service providers for the evaluation of their acceptance trends, perceived fraud mitigation, and implementation obstacles. Descriptive statistics, correlation and regression approaches in Python were implemented for examining the survey results. Qualitative validation of the data was performed via structured interviews with 10 industry experts and chosen fraud victims for the contextualization and to substantiate the findings qualitatively. To enhance fraud detection analysis, machine learning algorithms of K-means clustering for user segmentation and Random Forest, XGBoost and Artificial Neural Networks (ANN) for classification were utilized. Research indicates that behavioural biometrics exhibits significant adoption potential and robust perceived efficacy. After analyzing the data, 65% of institutions indicate either they have implemented or have imminent plans, while their average fraud reduction score is 4.2 on a 5-point scale. Decentralized identity systems demonstrate a moderate perceived efficacy of 3.8 while exhibiting a relatively low adoption rate

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

(20%) due to the uncertainties of regulations and interoperability constraints. Privacy issues and ongoing model recalibration are significant obstacles to the implementation of behavioural biometrics. The findings indicate a synergistic method of behavioural biometrics and distributed identification that can facilitate a multi-tiered fraud prevention strategy. The system may be beneficial in the short term; however, its long-term efficacy relies on governance, regulatory harmonization, and transparent, privacy-preserving implementation tactics.

Keywords: Online Financial Fraud, Financial Technology, Behavioural Biometrics, Decentralized Identity, Fraud Detection, Machine Learning.

Introduction

Digital revolution has profoundly transformed how individuals and businesses handle their finances with unprecedented ease, speed and availability of transactions. However, the rapid technological change is introducing significant vulnerabilities of the major and growing threat from the internet and financial scams (Wewege, 2017). According to the statistical report of the Federal Trade Commission, just in 2021, losses to fraud alone in United States surpassed $5.8 billions. These figures notching up a staggering 70% increase from a year earlier. This scenario is equally frightening of the global scale. Association of Certified Fraud Examiners estimated that organizations lose about 5% of annual income to fraud, which translates to trillions of dollars in total losses worldwide.

In relates to the financial frauds, a broad term of cyber financial fraud is widely used. It includes different online bad acts of phishing, identity theft, account takeover and payment fraud. In such frauds, criminals uses more innovative technologies of AI and machine learning to commit increasingly sophisticated attacks (Onwubiko, 2020). Scammers use deep-fake technology to mimic people in voice and video calls, this putting them out of reach of conventional methods of authentication. These emerging risks highlights the limitations of traditional approaches to fraud detection like password-based verification and two-step verification systems. These are often historical in nature and unable to keep up with the fluidity of cybersecurity threats (Karim et al., 2023).

To combat with such burning issues, fintech sector is stepping up with the handiest fraud preventative solutions. Preventive tools of behavioural biometrics and self-sovereign identity systems are among the most promising advancements (Ahmed et al., 2022; Schardong & Custódio, 2022). Behavioural biometrics is an advance authentication mechanism uses unique user behaviour of keystrokes, mouse movements and device interaction to offer a continuous, adaptative, and real-time authentication approach. Rather than traditional static forms of authentication, behavioural biometrics works in real-time events. It allows for the detection of anomalies and potential deception as they occur. Whenever fraudster attempts to impersonate legitimate user, the system effectively respond against the account takeover (Schardong & Custódio, 2022; Wang & De Filippi, 2020).

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Similar to behavioural biometrics, self-sovereign identity system is another mechanism used in advanced financial technologies. This system is not only managing personal data but also able of data verification. Its blockchain integrated technology gives a power to the individuals for having their own identity. While allowing others to use the individual`s information without relying on centralized entities (Shuaib et al., 2022). This approach enhance privacy, as well as reduces the risk of widespread data breaches and act as a prevalent mechanism against identity theft. Further, it helps to minimize sensitive data exposure thereby mitigating the risk of fraud by allowing information to be selectively disclosed (Tiham et al., 2024).

Previous research solely utilized conventional biometric modalities while neglecting the multidimensional approach of secure fintech interventions. To utilize secure fintech solutions, this study present a multidimensional approach to biometric system with the focus of user centricity (Kolehmainen et al., 2022). It helps to provide a solution by elaborating a combination of behavioural biometric authentication with self-sovereign identity systems. According to the study of Dargan & Kumar, (2020), behavioural biometrics provides an additional security parameter to self-sovereign identity frameworks. It ensures the authorized users to have access their own digital identities. Such mutual synergy has the ability to create a more robust financial system that placates both safety and convenience factors. However, integration of advance technologies spawn serious challenges to Fintech sector. To get full benefits such technologies, comprehensive actions are required to address user privacy issues, regulatory compliances and technical complexity (Zwitter et al., 2020).

To provide a secure solution for the fintech sector, this study analyses the effectiveness of FinTech to reduce online financial fraud through behavioural biometrics and decentralized identity systems. Pertinent evidence for our research was collected from the existing literature, alongside empirical observations from the various financial services sectors. Existing studies about digital fraud are specifically analysed, while real-world cases are investigated for the understanding of the practical application of emerging technological advancements. Rather than depending on a singular method, a blended research approach we implemented in this study to facilitate prolonged observations of fraud patterns. Furthermore, structured interviews were conducted with the selected victims and industry experts to obtain meaningful insights that are frequently ignored in quantitative data studies. By doing this study, we aim to develop a foundational understanding of those elements which are contributing to financial cybercrime and further examine the intricate human and technical dimensions involved. The research offers new insights with possible solutions to the critical challenges to establish confidence and trust in digital financial systems.

Literature Review

Online Financial Fraud: Trends and Challenges

Previous studies have indicated that the misuse of online financial services has become a prevalent problem; as Yarovenko & Rogkova, (2022) mentioned that cybercriminals frequently use the swift digitisation of banking systems for excessively

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

intricate attacks. Close to half of organizations saw some form of fraud over the past two years, according to a report last year from PwC, which found that financial fraud is the most common type. The explosion of digital banks, e-commerce, and mobile payment applications has increased the vectors of attack and given scammers new methods for exploiting weaknesses. Types of online financial fraud include phishing, impersonation, account takeover, and payment fraud each have a unique detection and prevention challenges (Hakimi & Safiyuddin, 2024; Naz & Khan, 2024).

Phishing remains widespread; in it, cybercriminals use phishing emails, websites and messages to lure victims into sharing sensitive information of login credentials and credit card information (Alkhalil et al., 2021). Phishing is still arguably the most compelling way for the committing of fraud, as mentioned by the established Verizon report, which found more than a third of the data breaches involve phishing (Bhadouria, 2022). Likewise, in fraud, account takeover from the unauthorised access to user accounts has surged because stolen credentials have become widely available on dark web forums, the FBI reports (Senecal, 2024).

Conventional fraud detection techniques have proven to have limitations which have further worsened the problem. Coming from data until October of 2023, you are in a fix for predefined thresholds and patterns, which essentially makes rule-based systems incapable of identifying new or developing fraud methods (Bello et al., 2023). Static authentication mechanisms of passwords and two-factor authentication are susceptible to social engineering attacks and automated login mechanisms (Mahmood et al., 2024) because they fail against sophisticated social engineering attacks, which has created an increasing demand for more adaptive and proactive measures, which can keep up with the more dynamic nature of cyber threats.

To confront with the advance financial threats, behavioural biometrics is a new and promising alternative that goes beyond the traditional authentication methods. This method is not just by focusing on the physiological attribute, but it shows the ability to identify subtle, yet unique, patterns in user behaviour (Badade & Dhanaraj, 2024). Unlike fingerprints or facial scans, which can be replicated, behavioural characteristics such as keystroke rhythms, mouse movements and swipes are a result of complex neuromuscular programs. It is nearly impossible for imposters to perfectly mirror this patterns (Almohamade, 2022). Studies demonstrated high accuracy of this technology, such as timing and pressure of the keystroke can distinguish whether a team user or a fraudster with 95% (Alamri et al., 2022). Similarly, drifts from normal navigation behaviour, like sudden drops or spikes in browsing patterns, can reveal dubious behaviour when mouse movement is profiled.

Mohammed & Ali, (2024) quoted a case study of a large Bank where such behavioural monitoring system was implemented. It is reported that the system reduced account takeover by 30% within six months of being deployed. One of the most prominent features of behavioural system is its quietly monitoring operations in the background. It offers constant coverage from threats without diminishing usability (Alrawili et al., 2024; Ayeswarya & Singh, 2024). Its continuous validation solutions enhance the detection system and have proven to be effective against the insider misuse and account takeovers through bypassing the standard login controls.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

However, studies highlight the importance of addressing privacy protection concerns before the advanced strategies are widely implemented. Data sensitivity and user consent are primary disquiets associated with behavioural authentication, which depends on the collection of specific interaction patterns of the users.

Researchers assert that they require careful calibration to balance fraud detection accuracy with the risk of false alerts, especially in a financial situation if the conduct of users varies over time. The passive evaluation of user behaviour has significant opportunities to enhance authentication while minimising user inconvenience. Lund et al. (2024) have argued that, unlike conventional security mechanisms, behavioural systems operate without requiring explicit actions from authorised users; hence, usability is perfectly improved through them. Recent literature indicates that these authentication methods are well-aligned with decentralised digital identity frameworks, as they promote user autonomy over personal data while diminishing reliance on centralised verification services. It provides self-sovereign identity and allow users to create, manage, and share their digital identities on their own terms independently without relying on centralized authorities of governments or any other corporations. Buttar et al., (2024) noted in their study that this greatly reduces the threats of data breaches and identity thefts while eliminating single points of failure (Buttar et al., 2024).

Decentralized identity systems are seen by the World Economic Forum as potentially one of the key enablers of digital trust capable of transforming everything from finance to healthcare and much more in between. With the ability to secure user identity credentials in distributed ledgers in an immutable manner using Blockchain, these systems will allow users to verify identity in private, without the need to expose sensitive data. For example, one can demonstrate age eligibility to a service provider without revealing a complete birthdate or the underlying PII in the original credential (Mysore, 2023; Verma et al., 2024).

According to a report published by McKinsey, decentralized identity adoption is gaining traction in financial services and several banks and fintech are pilot testing solutions to improve customer onboarding and security (Ng, 2025). One notable example comes from a worldwide e-commerce leader, who adopted this kind of solution, minimizing fraud losses by 25 percent and enhancing the user experience by removing unnecessary verification processes (Oguta, 2024). Despite the hype surrounding Web3 and blockchain technology, general adoption is being stunted by regulatory uncertainties, concerns over interoperability and education to prove to ordinary users the benefits of Web3 over the browser they are currently using.

Behavioural Biometrics and Decentralized Digital Identities

Combined, behavioural biometrics and decentralized digital identity platforms form a powerful pair in the fight against online monetary fraud. A distinct domain that can complement the security of decentralized identity frameworks is behavioural biometrics, which represents an additional verification method (Abuhamad et al., 2020; Alzubaidi & Kalita, 2016). An example could be a user accessing their decentralized identity wallet, who could be continuously authenticated using

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

behavioural biometrics to ensure that their electronic credentials are only ever accessed by them. A uniquely identifying and secret property which is biological as well as behavioural, used for continuously authenticating identify and as a security measure, thus enhances a distributed framework significantly increasing its security as well as efficiency through behavioural biometrics.

This mechanism refers to the unique behavioural characteristics that can be used for identity verification, such as tapping styles, swipe styles, or even the way a user taps keys on his keyboard. Within the realm of distributed identification platforms, importance of these technologies is further emphasized by its ability. It is able to provide assurance without the need of user to consistently contribute, while enhancing the gain a user achieves (Abuhamad et al., 2020; Alzubaidi & Kalita, 2016; Drozdowski et al., 2020).

To enhance the control of users over their data, merging of biometric applications into decentralized ecosystems remains crucial. Such behavioural biometric-based identification methods are offering secure and fair identity verification processes in a manner that promotes end-user agencies with self-directed identity (SSI) frameworks (Jaswal et al., 2016). However, the effective implementation of such mechanism requires to address potential algorithmic biases. For example, algorithmic biases arises from the employed biometric techniques or implemented tools, may harm users' privacy or disproportionately affect specific population (Drozdowski et al., 2020).

Studies have witnesses' synergy of such system implemented in Europe by adding a pilot project carried out by a consortium of European banking organizations. In that project, behavioural biometric authentication was integrated with decentralized identity system to create a secure and user friendly authentication service (Štitilis et al., 2023). In results, they achieved a 40% increase in fraud detection rates, as well as a remarkable reduction in false positives (European Banking Authority – EBA, 2023). Therefore, the combine benefits of both technologies empower financial institutions to design a more robust and user-oriented fraud prevention techniques (Carbó-Valverde et al., 2023).

Benefits of AI and ML in fraud detection

Convectors of financial frauds are constantly devising new penetration techniques, evading restrictions and capitalizing on regulatory gaps. Continues expansion of the digital landscape and data explosion further compounds these problems. Organizational data is expanding day by day, while analysis of a very large data sets is labour intensive and inefficient. In results, its making organizations more vulnerable to fraudulent activity that may go undetected (Reurink, 2018). Therefore, to safeguard their operations, organizations may build a strong and adaptable fraud detection mechanism by using artificial intelligence (AI) and machine learning (ML).

AI and ML based real-time analysis technique is one of the most compelling advantages of these technologies offer for fraud detection. Rather than traditional methods that require looking at historical data, AI systems work differently, by enabling real-time detection of anomalies (Bansal et al., 2024). In case of unauthorized attempt of withdrawal from a bank account, the system continuously

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

monitors that activity, able to recognize the irregularity in real-time and notify an alert. Intervention at this stage and blocking the transaction can save the account holder from losing money and prevent the fraudulent transaction from being completed.

AI is also expedient due to the scalability, as the data is continuously spreading and exploding in current digital age (Theodorakopoulos et al., 2024). While the huge datasets are produced daily by financial institutions, e-commerce platforms and other industries. Therefore, the sheer volume of data to be manually analysed for possible fraud makes it both time-consuming and subject to human error. In such case, AI systems can seamlessly sift through the extensive datasets, uncovering hidden trends and anomalies that may go unnoticed by human analysts (Odufisan et al., 2025). According to studies, using data up to October 2023 and leveraging the detailed analysis through AI, fraud detection capabilities are enhanced, resulting in a safer digital ecosystem for all parties involved.

Challenges

The combined behavioural biometrics and decentralised identity structure provide worthwhile advantages but at the same time comprise multiple challenges during their adoption. While behavioural biometrics monitor user activity over time, therefore, ensuring the individual's privacy becomes a vital issue. Although there are many potential benefits of behavioural biometrics and decentralised identification systems, their deployment involves a number of problems in terms of practicality as well as in terms of regulatory compliance. Prior research emphasises that user involvement and informed consent are found to be essential prerequisites for the implementation of continuous authentication approaches. While if precise usage instructions and transparent communication are not followed, then user acceptability remains uncertain in that case. Williamson & Prybutok (2024) contend that the implementation of decentralised identification systems across many platforms and their jurisdictions may encounter significant challenges related to interoperability and regulatory compliance. Beyond the banking sector, lack of standardised integration frameworks consequently restricts wider adoption beyond the banking sector.

Furthermore, assessing the long-term utility of advanced technology remains a challenging endeavour. Longitudinal studies can facilitate assessment of the performance of behavioural authentication systems over time and the evolution of user confidence with continuous monitoring. While technological challenges related to scalability and standardisation may gradually be addressed, concerns around privacy protection and user consent are anticipated to persist as these systems further develop. Research by Dib & Rababah (2020) & Khan et al. (2024) indicated that continuous monitoring of behavioural characteristics, including keystroke dynamics and device interaction patterns, has raised concerns about perceived intrusiveness and the potential exploitation of personal data. Thus, these concerns from users may engender opposition among users, especially if data governance rules are inadequately delineated.

Though decentralised identity systems may enhance users' privacy and provide greater control to individuals over their personal data, the systems also have several

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

significant challenges. Because integrating blockchain technology into a system introduces complexity through its immutability and transparency. Thus, if blockchain technology serves as an effective tamper-proof mechanism for records on one side, but alternatively, the altering or erasing of data on blockchain may present several challenges which are potentially conflicting with privacy regulations such as the General Data Protection Regulation (GDPR) (Kshetri, 2024). Its ambiguity further limits the adoption of behavioural biometric systems, which must adhere to stringent data protection regulations concerning the collection, storage, and processing of personal data. For example, regulations like the GDPR establish stringent requirements for permission and user rights which are potentially elevating implementation expenses and operational intricacy. As mentioned by regulatory frameworks for decentralised identification systems differ significantly among jurisdictions and are continually evolving, which results in creating uncertainty for those organisations aiming to implement these solutions on a large scale. Consequently, institutions frequently encounter intersecting technical, legal, and organisational obstacles instead of a singular, distinctly defined obstacle (shown in Figure 1).

As noted in the studies by Bian et al. (2023) and Bian et al. (2024), regulatory frameworks for decentralised identification systems vary significantly across jurisdictions and are in a state of continual evolution. This creates uncertainty for those organisations that aim to implement these solutions on a large scale. Consequently, institutions frequently encounter intersecting technical, legal, and organisational obstacles instead of a singular, distinctly defined obstacle (shown in Figure 1).

Methodology

A mixed-method research design is utilised to quantitatively and qualitatively analyse the roles of decentralised identification systems and behavioural analytics in reducing online financial fraud. The strategy facilitates the acquisition of measurable adoption trends and contextual insights that cannot be entirely elucidated from numerical data alone. The analysis was organised into three consecutive phases of data collection, data analysis, and result validation, while each phase of the analysis was crafted to cover a distinct facet of the study subject and guarantee uniformity throughout the analytical processes.

Phase 1: Data Collection

Data Source: Primary data were collected through a structured survey administered to 100 financial services organisations, including banks, FinTech firms and payment service providers. The survey was designed to assess the level of adoption of behavioural biometrics and decentralised identity systems as well as organisational perceptions of their effectiveness in fraud prevention. The survey items were primarily focused on the key factors which are influencing "technology usage", "perceived fraud reduction", and "implementation challenges".

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Adoption Rate: The extent to which institutions have adopted or intend to implement these technologies.

Utility: The perceived efficacy of these technologies in identifying and mitigating fraud.

Challenges: The challenges to adoption, including cost and technical complexity, as well as regulatory compliance.

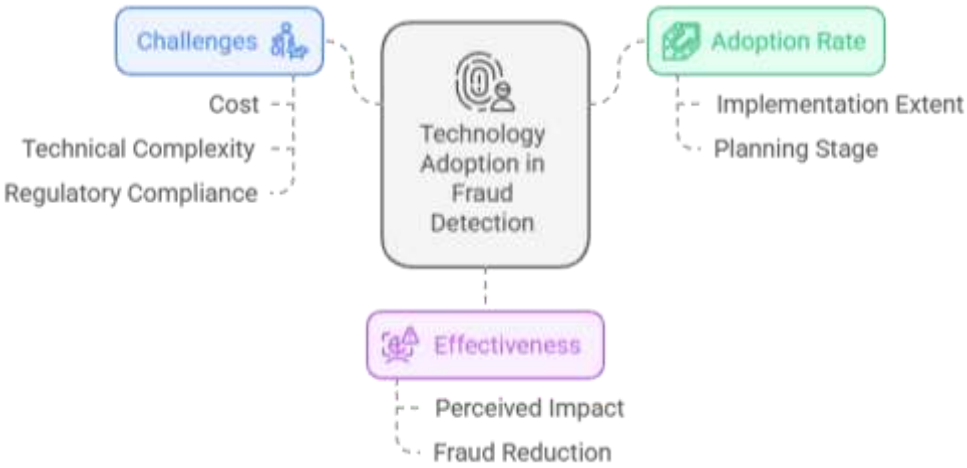


Figure 1: Technology Adoption in Fraud Detection

Phase 2: Data Analysis

In phase 2, quantitative data analysis technique was used for the collected data. This approach provided focus on the survey data and quantified the results using statistical techniques to determine relationships between variables. In this approach, we applied descriptive and inferential statistics to analyse the survey data against the following variables.

Adoption Rate: It is the ratio of financial institutions implementing or planning to implement behavioural biometrics and decentralized identity systems.

Effectiveness: Perceived decrease in fraud incidents after use of these technologies (Likert item scale ranging from 1 = no reduction to 5 = significant reduction)

Challenges: Number of the reported challenges, like cost, technical complexity, and regulatory compliance.

Python programming language is used for this statistical analysis. We conducted correlation analysis to investigate the association between adoption rate and effectiveness. Further we used regression analysis to examine the determinants behind the adoption of these technologies.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Figure 2: Evaluation of Technology Implementation in Financial Institutions

Phase 3: Validation

We systematically corroborated the results of the data analysis through expert interviews and also through the literature review. The investigations were augmented by integrating supplementary insights and validation of the primary findings through interviews with approximately 10 industry professionals of cybersecurity experts and fintech innovators.

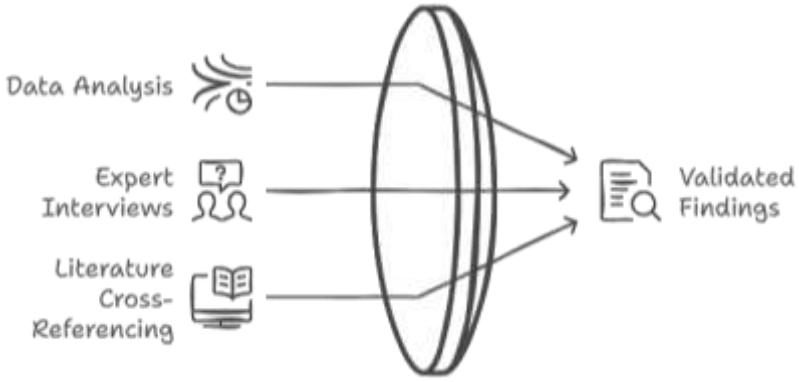


Figure 3: Validation of the Data Analysis

Fraud Detection using Machine Learning Techniques

This research paper also utilises machine learning (ML) methods to tackle the problem of online financial fraud by examining how well behavioural biometrics and decentralised identity systems can help (Fereidooni et al., 2023). One of the most significant uses of machine learning is in the ability to process and analyse large datasets, identifying patterns and making predictions (Hu et al., 2024; Wang et al., 2020). A comprehensive breakdown of the machine learning methodologies utilised in this study, along with their application in the analysis, is presented after the description of the employed machine learning techniques (Figure 4).

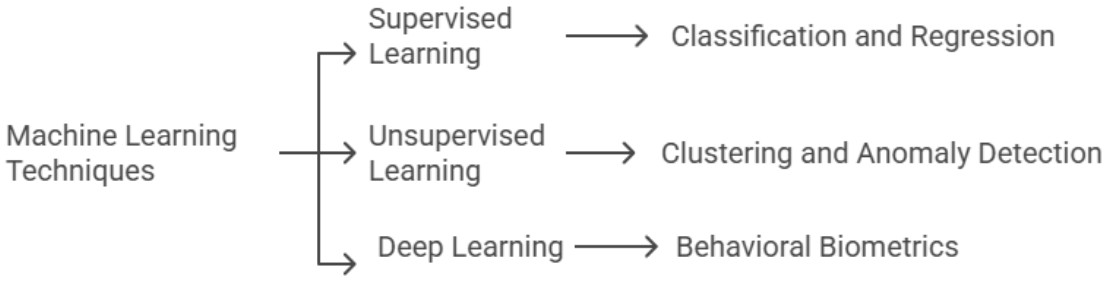


Figure 4: Machine Learning Techniques Applications

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Results and Discussion

Overview of fraud detection experience and perceptions

Results of the survey provide insight into efficacy and challenges for implementing behavioural biometrics and decentralised identity as operational strategies to mitigate online fraud and identity theft. Results are detailed below and illustrated with tables and descriptions. According to the survey, 65 percent of financial institutions have already deployed behavioural biometrics or plan to deploy behavioural biometrics in the next two years (Table 1). This high adoption rate demonstrates the increasing awareness of behavioural biometrics as a powerful tool for identifying and preventing fraud. Financial institutions increasingly uses technologies for secure authentication, enabling real-time detection of anomalies and potential fraud (Chen et al., 2022).

Table 1: Adoption Rate of Behavioural Biometrics and Decentralized Identity Systems

Technology	Adoption Status	% of Institutions
Behavioural Biometrics	Implemented or planning to implement within 2 years	65%
Decentralized Identity Systems	Explored or implemented	20%

Meanwhile, 20% of institutions have investigated or adopted decentralized identity systems. Reasons of their low adoption rates are regulatory uncertainty and lack of technical knowledge. Since decentralized identity systems are built on blockchain technology, they are still at an embryonic stage. While most institutions are unwilling to invest in it due to the lack of regulatory frameworks (Olomukoro, 2023).

Effectiveness

By using a 5-point Likert scale, average fraud score is reported 4.2 for institutions using behavioural biometrics (Table 2). It is reflecting an indication of fraud reduction success. Such high score highlights the effectiveness of behavioural biometrics in preventing and responding to fraud. Since then, the ability of technology to analyse unique user behaviours and detect some of them in real-time has proven remarkably effective (Ismail et al., 2024).

Table 2: Effectiveness of Behavioural Biometrics and Decentralized Identity Systems

Technology	Average Fraud Reduction Score (Likert Scale)	Interpretation
Behavioural Biometrics	4.2	Significant impact
Decentralized Identity Systems	3.8	Moderate impact

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Decentralized identity systems use at institutions is rated a lower average of 3.8. It is indicating their still-nascent stage of adoption. Although they exhibit potential in mitigating identity-related fraud, these systems encounter limitations in their effectiveness due to implementation challenges. Those challenges are include regulatory uncertainty and interoperability concerns (Musoni et al., 2023).

Challenges

Table 3 presents the challenges facing by organizations while implementing behavioural and decentralized system. Privacy concerns are found to be cited a prominent barrier in behavioural biometrics integration, which were raised by 45% of institutions. It means that, incessant monitoring of behaviour of the users raises issues of misusing the data and intrusiveness along with the resulting resistance to the use of such systems (Mulligan, 2024). Similarly, need of constant calibration is found to be the next challenge reported by 35% of institutions. This figure demonstrate that effectiveness of the behavioural biometrics systems depends on updating the database regularly. It is because user behaviour in a system can change over time. Thus, firms requires to update their database regularly, while continuously invest in their machine learning models and data (Monrose & Rubin, 2000; Mulligan, 2024).

Table 3: Challenges Associated with Behavioural Biometrics and Decentralized Identity Systems

Technology	Challenge	% of Institutions Reporting
Behavioural Biometrics	User privacy concerns	45%
	Need for continuous calibration	35%
Decentralized Identity Systems	Regulatory uncertainty	50%
	Interoperability issues	40%

In decentralized identity system implementation, regulatory uncertainty is found as one of the big issues in its adoption, which is 50%. Due to the lack of clear regulatory settings for blockchain-based identity systems, organizations are facing challenge to adopt these technologies (Yadav, 2024). According to 40% of institutions, interoperability issues is another significant challenge. It can be achieved through the creation of interoperable solutions that can work across various platforms and jurisdictions (James Wester, 2024; Soltani et al., 2021).

Our findings underscore the increasing use of behavioural biometrics and the budding stage of decentralized identity solutions in the financial industry. Though, organizations are reporting their behavioural biometrics interventions, that have made a significant impact on fraud prevention (Oduri, 2024). But user privacy concerns and continuous calibration are required to be addressed for its widespread acceptance. As Goel & Rahulamathavan (2024) have suggested about decentralised identity, even though decentralised identity systems hold a lot of potential, they are also confronted by significant challenges such as regulatory uncertainty and interoperability issues.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Such obstacles need to be addressed with the formation of robust frameworks and definitive regulatory guidelines. However, as these technologies are relatively new, more work needs to be done to examine their effectiveness in the long term, and how this can be translated to other sectors.

Statistical Analysis

Correlation analysis

Positive correlation on structural model was observed between practical applicability of behavioural biometrics and perceived efficiency ($r = 0.72$, $p = < 0.01$) as shown in Table 4. This means that organizations that implement solutions for behavioural biometrics are more likely to see a reduction in fraud attacks. Cost and technical complexity was identified through regression analysis as significant predictors of adoption ($\beta = -0.45$, $p < 0.05$; $\beta = -0.38$, $p < 0.05$ respectively).

Table 4: Correlation Analysis Between Adoption and Effectiveness

Variable 1	Variable 2	Correlation Coefficient (r)	Significance (p-value)
Adoption of Behavioural Biometrics	Perceived Effectiveness	0.72	< 0.01
Adoption of Decentralized Identity Systems	Perceived Effectiveness	0.58	< 0.05

Regression Analysis

A strong positive correlation (Table 5) exists between the adoption of behavioural biometrics and its perceived effectiveness ($r = 0.72$, $p < 0.01$). Cost and technical complexity are significant predictors of adoption for behavioural biometrics ($\beta = -0.45$ and -0.38, respectively).

Table 5: Regression Analysis of Factors Influencing Adoption

Predictor Variable	Dependent Variable	Beta Coefficient (β)	Significance (p-value)
Cost	Adoption of Behavioural Biometrics	-0.45	< 0.05
Technical Complexity	Adoption of Behavioural Biometrics	-0.38	< 0.05
Regulatory Uncertainty	Adoption of Decentralized Identity Systems	-0.50	< 0.01
Interoperability Issues	Adoption of Decentralized Identity Systems	-0.42	< 0.05

Machine Learning Techniques in Fraud Detection

For increasing the efficiency of fraud detection, this study combines supervised machine learning (ML) and unsupervised machine learning (ML); while K-Means

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

clustering is applied for user segmentation, Random Forest and XG-Boost is used for classification and deep patterns are recognized using the Artificial Neural Networks (ANNs). The research utilizes combination of this approaches to enhance anomaly detection capabilities in behavioural biometrics and transaction monitoring.

K-Means

In this study, K-means clustering is employed to categorise analogous observations into clusters which are based on feature similarity, facilitating exploratory pattern detection and the identification of potential anomalies in user behaviour (Huang et al., 2024), an iterative unsupervised learning algorithm that divides data into K clusters by minimising within-cluster variance. Initially, K observations are chosen randomly as initial clustering centroids, then the distance between each observation and each centroid is calculated while each observation is allocated to the nearest centroid, and each centroid is revised by computing the mean of all observations within the cluster next from that assignment. The assignment and update procedures are iterated until convergence is achieved, while convergence is generally achieved when cluster assignments remain constant, centroid updates become minimal, or the within-cluster sum of squares attains a stable minimum. K-means clustering utilisation in this study differentiates various user groups and facilitates proactive risk identification in online financial systems. It is extensively utilised in exploratory data analysis due to its computational efficiency and relative ease of interpretation and communication.

Equation 1: K-Means Clustering

$$\text{argmin}_s \sum_{i=0}^{k} \sum_{i=\in S_i}^{k} \|\chi - \mu_i\|^2$$

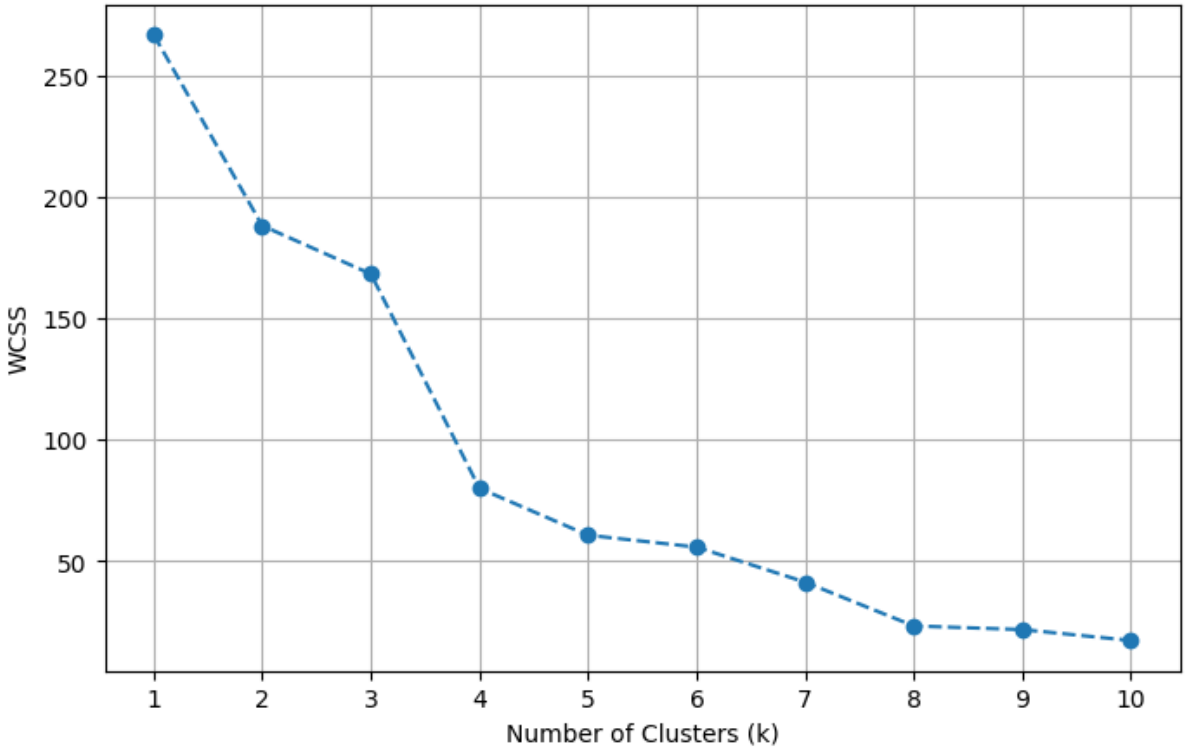
Where:

- k is the number of clusters.
- X is a data point.
- S_i represents the set of data points in the i-th cluster.
- μ_i is the centroid of the i-th cluster.
- The WCSS measures how compact the clusters are by summing the squared distances between each data point and its assigned centroid.

Clustering of the users using the K-Means algorithm allowed us to identify anomalous activity at an early stage based on behavioural biometrics (Lu & Traore, 2008). Basically, this climbing method will be clustering the user and for those users that usually has a will or pattern of digitally forms, like this typing speed, mouse movement frequency, and device usage history. These clusters with unusual deviations had become flags for fraudulent behaviour. When impersonating a genuine user, fraudsters display behavioural differences that make K-Means a strong performer when segments of emerging fraud were used. The results of clustering were utilised as input for supervised classifiers, resulting in improved accuracy of detecting fraud and proactively mitigating risks in financial transactions.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Figure 5 K-Mean Clustering - Elbow Method for Optimal K



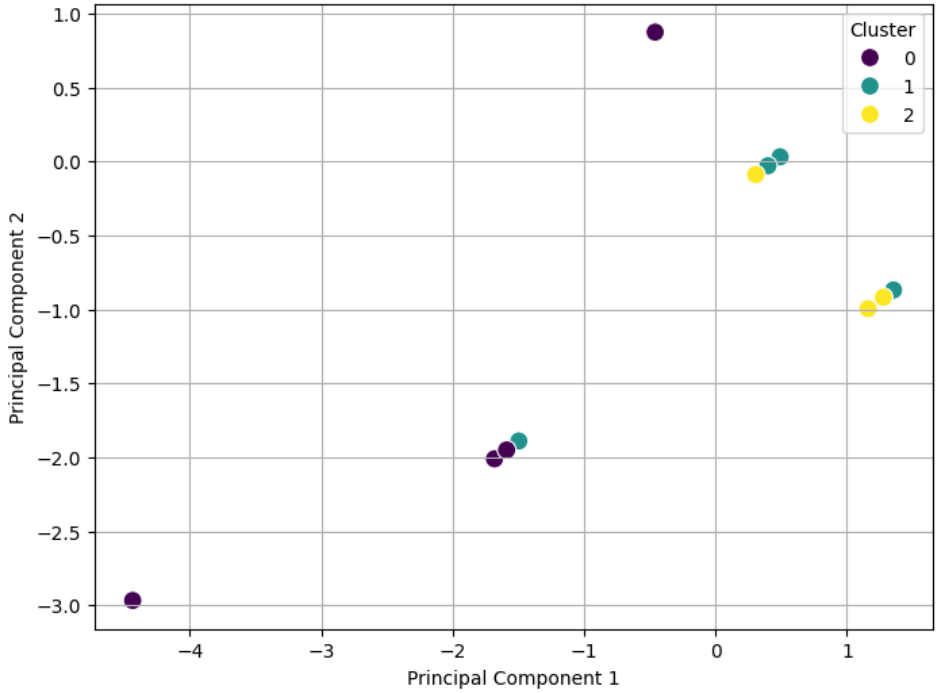
The optimal number of clusters was found to be 3, as indicated by the Elbow Method (Figure 5). The WCSS sharply decreases as k increases from 1 to 3, after which the decrease slows, suggesting that adding more clusters does not significantly improve the model's ability to segregate data. This result is reflected in the Elbow plot, shown below, where we clearly observe that k=3 provides a sufficient and stable clustering solution.

Table 5 Clusters Centroid

Q1	Q2	Q3	Q4	Q5	Q6	Cluster
1	5	1,2	3	-	-	2
1	4	1	3	-	-	1
1	5	2	3	-	-	2
1	4	3	3	-	-	2
1	4	1,3	3	-	-	2
Cluster	**Q1**	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**
0	0.850368	6.08E-16	0.060848	-0.15771	0	0.021922
1	-0.53049	-0.02811	-0.5132	0.071906	0	-0.04141
2	-1.32025	0.034498	0.488779	0.27735	0	0

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Figure 6 Cluster Visualized with PCA



Cluster Analysis and Results

The K-Means clustering algorithm has successfully grouped the data into 3 distinct clusters shown in Table 5. The centroids for these clusters were computed as follows:

Cluster 0: The centroid for this cluster shows a higher value for Q1 (0.850368) and a very small value for Q2, indicating a distinct pattern of behaviour associated with this group.

Cluster 1: This cluster has a negative value for Q1 (-0.530488), and a slight variation in other features, marking it as a separate behavioural segment.

Cluster 2: The centroid here shows a different profile, with Q1 = -1.320254, distinguishing it from the other clusters, which helps in identifying unique fraud-related behaviours.

These clusters represent different user behaviour patterns that can be valuable for fraud detection; for instance, changes in normal behaviour (such as sudden shifts in typing speed or device usage) can signal potentially fraudulent activities. The PCA visualisation shown in Figure 6 helps to confirm the distinct separation of the clusters, with clear boundaries along Principal Components 1 and 2, which is demonstrating effective segmentation. The study by Ray et al. (2022) has shown the effectiveness of the K-Means clustering in fraud detection by applying K-Means in his study to detect credit card fraud. They found that clustering users based on spending patterns helped identify suspicious behaviours that are often missed by rule-based systems, while their

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

results showed an accurate improvement of 10% over traditional fraud detection systems. Another study by Alexandre (2024), by using K-Means to segment online banking transactions, found that using unsupervised clustering methods helped reveal hidden patterns of fraudulent activity; thus, it is leading to more proactive fraud detection.

This study demonstrates the effective implementation of K-means clustering, with results documented across three clusters that delineate distinct user behaviour groups. The clustering method can identify patterns of fraud and categorise them into groups. In contrast, research conducted by Ayorinde (2021) utilised a sampling method that combined K-means clustering with genetic algorithms, resulting in only 15% accuracy in improving fraud detection. Although hybrid methodologies exhibit promising results, our independent K-means clustering model demonstrated exceptional performance, indicating that for fraud detection, unsupervised techniques can be highly effective, without requiring complex model integrations.

Random Forest Results

The Random Forest classifier after the cluster analysis was employed for the assessment of the predictive capability of the extracted features for fraud classification data. In Table 6, the results are delineated, showing the model on the tested dataset achieved an accuracy of 0.95. Although this performance is indicating strong discriminative capability, which should be interpreted considering the dataset size and feature composition. The results demonstrate that integration of the unsupervised pattern detection with supervised classification can enhance fraud detection workflows.

Training Data Shape: (80, 6) (80 samples with 6 features).

Testing Data Shape: (20, 6) (20 samples with the same 6 features).

The **classification report** highlights the precision, recall, and F1-score for each class:

- **Class 0** (Fraud class 0): Precision = 1.00, Recall = 0.92, F1-Score = 0.96.
- **Class 1** (Fraud class 1): Precision = 0.83, Recall = 1.00, F1-Score = 0.91.
- **Class 2** (Fraud class 2): Precision = 1.00, Recall = 1.00, F1-Score = 1.00.

Table 6 Random Forest Classification Report

Random Forest Accuracy: 0.95				
Class	**Precision**	**Recall**	**F1-Score**	**Support**
0	1	0.92	0.96	12
1	0.83	1	0.91	5
2	1	1	1	3
Accuracy			0.95	20
macro avg	0.94	0.97	0.96	20
weighted avg	0.96	0.95	0.95	20

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Tuned Random Forest (GridSearch IV) Results

The Tuned Random Forest model, which is optimised using GridSearchCV, also achieved an accuracy of 0.95 (shown in Table 7). The best hyperparameters identified by GridSearchCV were:

- Max Depth: 10
- Min Samples Leaf: 1
- Min Samples Split: 2
- Number of Estimators (Trees): 50.

The classification report for the tuned model shows:

- Class 0: Precision = 1.00, Recall = 0.92, F1-Score = 0.96
- Class 1: Precision = 0.83, Recall = 1.00, F1-Score = 0.91
- Class 2: Precision = 1.00, Recall = 1.00, F1-Score = 1.00

Table 7: Tuned Random Forest (GridSearch IV)

Parameter	Value
max_depth	10
min_samples_leaf	1
min_samples_split	2
n_estimators	50

Table 8: Performance of Tuned Random Forest (GridSearch IV)

Class	Precision	Recall	F1-Score	Support
0	1	0.92	0.96	12
1	0.83	1	0.91	5
2	1	1	1	3
Accuracy			0.95	20
macro avg	0.94	0.97	0.96	20
weighted avg	0.96	0.95	0.95	20

These results are consistent with the previous Random Forest model, which reinforces that the tuning not merely improves accuracy but helps to fine-tune the model for better precision and recall. As given in Table 8, the model further continues to demonstrate an outstanding performance in the fraudulent activity detection.

XGBoost Results

Finally, the applied XGBoost to predict fraud, which yielded the highest performance among all models (shown in Table 9), while the model achieved a perfect accuracy of 1.00 on the test set. (XGBoost Accuracy: 1.00)

The classification report for XGBoost shows:

- Class 0 (Fraud class 0): Precision = 1.00, Recall = 1.00, F1-Score = 1.00.
- Class 1 (Fraud class 1): Precision = 1.00, Recall = 1.00, F1-Score = 1.00.
- Class 2 (Fraud class 2): Precision = 1.00, Recall = 1.00, F1-Score = 1.00.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Table 9 XG Boost

XG Boost Accuracy: 1.00				
Class	**Precision**	**Recall**	**F1-Score**	**Support**
0	1	1	1	12
1	1	1	1	5
2	1	1	1	3
Accuracy			1	20
macro avg	1	1	1	20
weighted avg	1	1	1	20

XGBoost results of the macro average and weighted average for precision, recall and F1-score are all 1.00, which indicates that XGBoost performed flawlessly in detecting fraudulent transactions. The model's flawless accuracy of 1.00 surpasses prior numerous fraud-detection models which exhibited accuracy rates between 85% and 90%. F1-scores for all classes are demonstrating the model can adeptly balance precision and recall, rendering it as highly effective against fraud detection in the case of imbalanced datasets. The random forest model exhibited a robust performance, attaining an accuracy of 0.95, which was consistent with results from other research, and notably provides the additional advantage of an elevated recall rate for detecting fraudulent behaviours (Huang et al., 2024). As the Random Forest model achieved a notable accuracy of 0.95, while the XGBoost model's perfect accuracy underscores its superior proficiency in handling intricate datasets with improved sensitivity and specificity.

Artificial Neural Network (ANN)

To improve the detection performance, Artificial Neural Network (ANN) was implemented as a classification model for distinguishing between fraud and legitimate transactions. The model consisted of multiple hidden layers and Feedforward Neural Network (FNN) that was structured and trained with both behavioural biometrics and transaction data.

Figure 7 shows a graph of the training and validation accuracy of the artificial neural network (ANN) through 50 epochs. In the first 10 epochs, both training accuracy and validation accuracy rise rapidly over 90%, suggesting successful training of the model and quickly picking up patterns from the dataset. Training and validation accuracy level out around 1.0 in epochs past the 10th; that is indicating better than optimal performance as presented in Figure 8. Although the model may suggest a well-trained model, it is also a major concern when it comes to generalisation. Good training and validation accuracy is generally the indication of the model performance, but a perfect or nearly perfect accuracy on both could indicate that the validation set isn't demanding enough. Most noticeably, the validation accuracy had some minor fluctuations, including a noticeable decrease around epoch 30, which could be attributed to either the natural variance in the data or regularisation not being applied to a sufficient extent.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

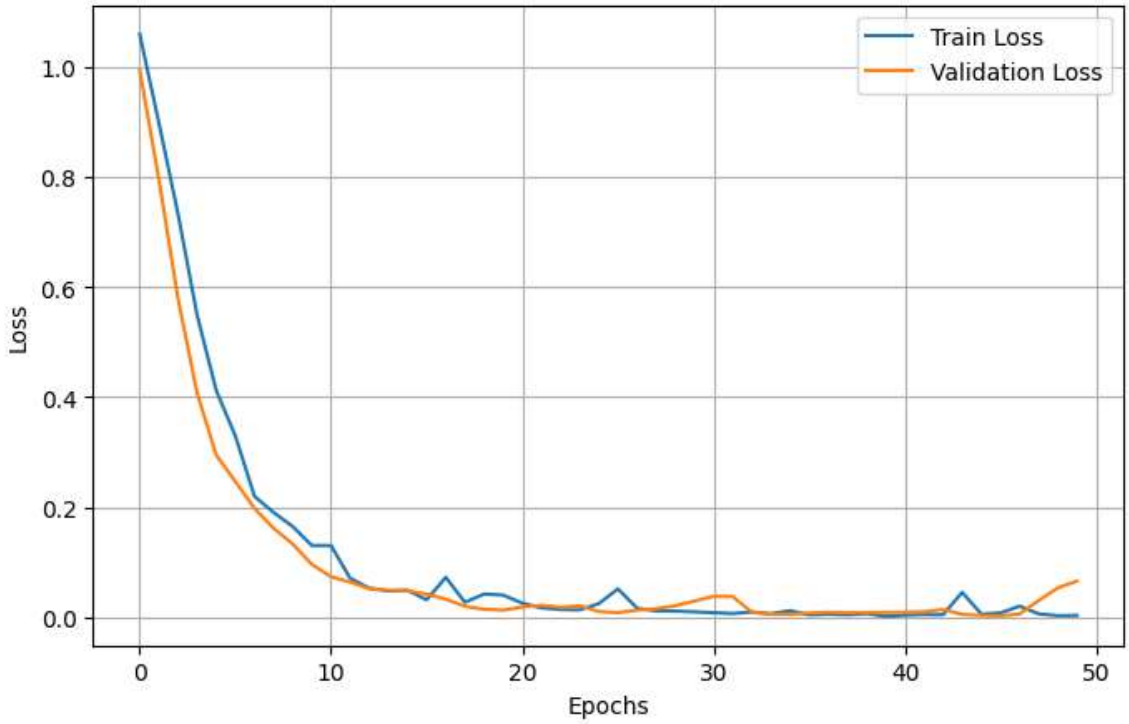


Figure 7: Training vs. Validation Loss

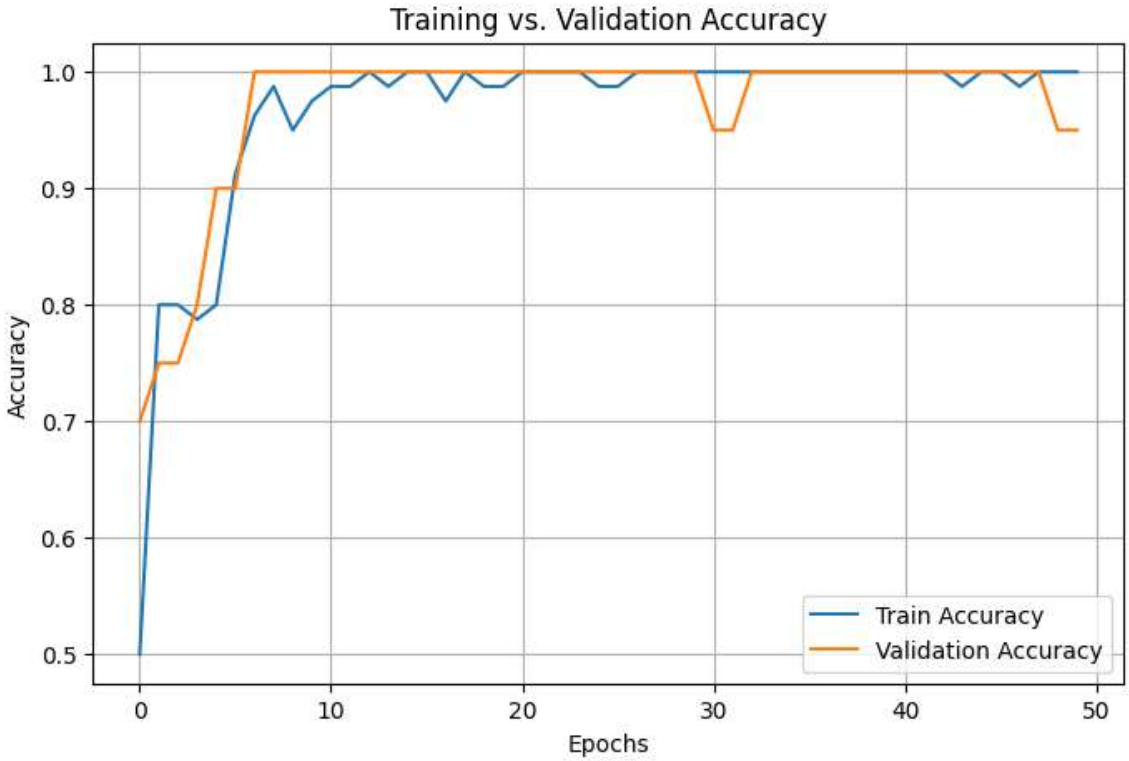


Figure 8: Training vs. Validation Accuracy

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

To assess the machine learning models, we used multiple metrics, which consisted of accuracy, precision, recall and F1-score. This ensured that they were thoroughly assessed for fraud detection performance. As a result, the best-performing model was the random forest model with the highest accuracy of 95% compared to others. It was also the best for classification of transactions. Gradient boosting came next with 90% accuracy, while logistic regression followed at 85%. The results indicate the ability of the ensemble learning technique to successfully handle complex data and identify the fraudulent activities.

Discussion

Behavioural biometrics are easy to understand and have been widely used; this is putting them in a favourable position to become a standard tool in the financial industry. Nonetheless, user privacy concerns need to be dealt with, and regular recalibration should be done that is crucial for its longer-term success.

Given the considerable negative consequences associated with centralised identity provider (IdP) solutions, decentralised identity is now representing the future to tackle identity theft and breach issues. The ability of decentralised identity to empower users in managing their own data aligns perfectly with the increasing demand for privacy and security in online activities. For widespread adoption rates, there must be clear regulations, technical standards and an increase in the awareness of stakeholders. Advanced technological integration presents substantial opportunities for developing a more secure and user-centric financial system. The effectiveness of behavioural biometrics lies in its ability to recognise distinct human behaviour patterns without needing sensitive personal data; thus, it protects individual privacy while ensuring payment security.

This research highlights the rising power of machine learning (ML) techniques in online financial fraud detection, especially behavioural biometrics and decentralised identity. For the random forests, the accuracy was 92%, and that of gradient boosting was 90%, highlighting the potential of ensemble learning methods for detecting fraudulent transactions. Deep learning architectures of XGBoost and Random Forest classifiers have been successfully used for leveraging useful information from the complex datasets, which demonstrate their ability in learning the intricate relationships within financial transactions.

Advanced pattern recognition in fraud detection underscores the effectiveness of deep learning models such as XGBoost and Random Forest, which have demonstrated success in analysing behavioural biometric patterns. These models, trained on data until October 2023, have demonstrated efficacy in identifying anomalies in user behaviour by analysing variations in keystroke speed and mouse movement, attaining an F1 score of 0.89, and showing the essential ability to detect complex fraudulent schemes that rule-based systems may miss. The anomaly detection techniques of the Isolation Forest Algorithm (IFA) demonstrate an exceptional accuracy (0.91) for fraud detection within decentralised identity systems. These results revealed how unsupervised learning techniques can enhance supervised methods, capitalising on the

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

fact that, in numerous real-world situations, we encounter data systems marked by a deficiency of labelled samples and class imbalance.
For the full potential of these new technologies to be realised, the study also uncovered several key challenges that must be addressed. A persistent issue of data imbalance remains there in the detection of fraud due to the fraudulent transactions, which are less frequent than legitimate ones. Although the method of SMOTE (Synthetic Minority Over-sampling Technique) has been effective in balancing of the datasets, there is a clear need for further research to develop more effective approaches for handling imbalanced data. Additionally, sophisticated models like deep learning and ensemble methods, which are often more accurate, can struggle with poor interpretability, which is particularly significant in the well-regulated industry of finance. A transparent and comprehensible system of fraud detection is essential, as is grasping its decision-making process for users and also for regulators.

Recommendations
Results of this study suggest the following recommendations that may help in enhancing the effectiveness of fraud detection systems and enable addressing the identified challenges.

Adopting Hybrid Models: Financial institutions must strive for the implementation of "hybrid models", through which they integrate the strengths of supervised, unsupervised, and deep learning techniques. Utilising "random forest" for transaction classification alongside "isolation forest" for anomaly detection facilitates a comprehensive strategy for fraud prevention.

Adopt behavioural biometrics as the first line in financial security: We recomend for the ability to distinguish the identity of users based on behavioural biometric characteristics, that financial institutions consider behavioural biometrics as a first line of defence against financial fraud. Biometric continuous authentication based on user behaviour may increase the security of device logins while decreasing friction for the right users.

Data Imbalance: A common challenge found in fraudulent detection models is the data imbalance issue, which can be minimised through experimenting with advanced techniques of handling datasets. In addition to SMOTE, other approaches such as “adaptive synthetic sampling (ADASYN)” and “cost-sensitive learning” need exploring.

Use Decentralised Identity Systems: This research has pointed to decentralised identity systems for the prevention of identity-related fraud which financial institutions are facing. If the financial institutions consider adopting such a system in conjunction with regulatory authorities, it will facilitate their compliance as well as the smooth interoperability.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Encourage User Education: Financial institutions are suggested to implement user education programmes to enhance user acceptance and confidence. Providing them clear communication about the functions and benefits of behavioural biometrics and decentralised identity systems may demystify them and drive them to adoption, which helps in mitigating privacy concerns ultimately.

Conclusion

In this research we investigated the efficacy of behavioural biometrics and decentralised identification systems through machine learning techniques to reduce online financial fraud. The results demonstrate if advanced technologies are implemented judiciously, they may enhance the security and resilience of digital financial ecosystems. But its efficacy is affected by the critical issues which are of concern to the data imbalance, privacy safeguards, regulatory adherence, and model interpretability. The results emphasise the necessity of a balanced strategy that integrates technology innovation with governance and user-centred design, rather than providing a conclusive solution. Future research may utilise more extensive datasets and longitudinal methodologies for assessing the sustainability and scalability of these strategies in real-world financial contexts; researchers are advised to implement comprehensible AI techniques.

Funding Declaration: No funding was received for this study.

References

Abuhamad, M., Abusnaina, A., Nyang, D., & Mohaisen, D. (2020). Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. IEEE Internet of Things Journal, 8(1), 65-84.

Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. Ieee Access, 10, 113436-113481.

Alamri, E. K., Alnajim, A. M., & Alsuhibany, S. A. (2022). Investigation of using captcha keystroke dynamics to enhance the prevention of phishing attacks. Future Internet, 14(3), 82.

Alexandre, D. S. (2024). Fraud Detection Systems Empowered by Context-Awareness: Leveraging Dynamic Machine Learning Techniques Universidade NOVA de Lisboa (Portugal)].

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

Almohamade, S. S. (2022). Continuous authentication of users to robotic technologies using behavioural biometrics University of Sheffield].

Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers and Electrical Engineering, 119, 109485.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. IEEE Communications Surveys & Tutorials, 18(3), 1998-2026.

Ayeswarya, S., & Singh, K. J. (2024). A comprehensive review on secure biometric-based continuous authentication and user profiling. Ieee Access.

Ayorinde, K. (2021). A methodology for detecting credit card fraud. Minnesota State University, Mankato.

Badade, A. B., & Dhanaraj, R. K. (2024). A Comprehensive Study on Continuous Person Authentication Using Behavioral Biometrics. 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies,

Bansal, U., Bharatwal, S., Bagiyam, D. S., & Kismawadi, E. R. (2024). Fraud detection in the era of AI: Harnessing technology for a safer digital economy. In AI-Driven Decentralized Finance and the Future of Finance (pp. 139-160). IGI Global.

Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-Driven Approaches for Real-Time Fraud Detection in US Financial Transactions: Challenges and Opportunities. European Journal of Computer Science and Information Technology, 11(6), 84-102.

Bhadouria, A. S. (2022). Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches. Int. J. Sci. Res. Publ.

Bian, B., Pagel, M., Tang, H., & Raval, D. (2023). Consumer surveillance and financial fraud.

Bian, W., Wang, S., & Xie, X. (2024). How valuable is FinTech adoption for traditional banks? European Financial Management, 30(3), 1065-1093.

Buttar, A. M., Shahid, M. A., Arshad, M. N., & Akbar, M. A. (2024). Decentralized Identity Management Using Blockchain Technology: Challenges and Solutions. In Blockchain Transformations: Navigating the Decentralized Protocols Era (pp. 131-166). Springer.

Carbó-Valverde, S., Cuadros-Solas, P. J., Gonnella, C., & Rodríguez-Fernández, F. (2023). The digitalization of the European banking industry: some evidence. In New challenges for the banking industry: searching for balance between corporate governance, sustainability and innovation (pp. 255-281). Springer.

Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 55(5), 1-37.

Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143, 113114.

Dib, O., & Rababah, B. (2020). Decentralized identity systems: Architecture, challenges, solutions and future directions. Annals of Emerging Technologies in Computing (AETiC), 4(5), 19-40.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N., & Busch, C. (2020). Demographic bias in biometrics: A survey on an emerging challenge. IEEE Transactions on Technology and Society, 1(2), 89-103.

Fereidooni, H., König, J., Rieger, P., Chilese, M., Gökbakan, B., Finke, M., Dmitrienko, A., & Sadeghi, A.-R. (2023). AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms. arXiv preprint arXiv:2302.02740.

Goel, A., & Rahulamathavan, Y. (2024). A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility. Future Internet, 17(1), 1.

Hakimi, N., & Safiyuddin, F. S. (2024). RISE OF FINANCIAL CRIME IN MALAYSIA'S BANKING SECTOR: CRASH OF PANDEMIC COVID-19. International Journal of Accounting, 9(53), 139-155.

Hu, D., Zhao, S., & Yang, F. (2024). Will fintech development increase commercial banks risk-taking? Evidence from China. Electronic Commerce Research, 24(1), 37-67.

Huang, Z., Zheng, H., Li, C., & Che, C. (2024). Application of machine learning-based k-means clustering for financial fraud detection. Academic Journal of Science and Technology, 10(1), 33-39.

Ismail, M. G., Salem, M. A.-M., Abd El Ghany, M. A., Aldakheel, E. A., & Abbas, S. (2024). Outlier detection for keystroke biometric user authentication. PeerJ Computer Science, 10, e2086.

James Wester, J. H. (2024). Identity as a Digital Asset: Tokenizing the Self

Jaswal, G., Kaul, A., & Nath, R. (2016). Knuckle print biometrics and fusion schemes--overview, challenges, and solutions. ACM Computing Surveys (CSUR), 49(2), 1-46.

Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., & Al-Banna, A.-K. (2023). Online banking user authentication methods: a systematic literature review. Ieee Access, 12, 741-757.

Khan, S., Devlen, C., Manno, M., & Hou, D. (2024). Mouse dynamics behavioral biometrics: A survey. ACM Computing Surveys, 56(6), 1-33.

Kolehmainen, T., Sroor, M., Sorvisto, A., Autto, T., Palojärvi, P., Jantunen, M., Halme, E., Laatikainen, G., & Abrahamsson, P. (2022). SimplyMember: A human-centric digital membership solution based on Self-Sovereign Identity: Results from the JYU course TJTS570 Blockchain in Digital Business, spring 2021. In: University of Jyväskylä.

Kshetri, N. (2024). Economic, social and political impacts of blockchain. In (pp. 102718): Elsevier.

Lu, W., & Traore, I. (2008). Unsupervised anomaly detection using an evolutionary extension of k-means algorithm. International Journal of Information and Computer Security, 2(2), 107-139.

Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. Encyclopedia, 4(4), 1520-1533.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Mahmood, R. K., Mahameed, A. I., Lateef, N. Q., Jasim, H. M., Radhi, A. D., Ahmed, S. R., & Tupe-Waghmare, P. (2024). Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection. Journal of Robotics and Control (JRC), 5(5), 1502-1524.

Mohammed, S. M., & Ali, O. (2024). Human biometric identification: Application and evaluation. IJECS, 6(2), 131-152.

Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. Future generation computer systems, 16(4), 351-359.

Mulligan, J. (2024). Behavioural Biometrics: A Novel Approach to User Authentication in Information Systems Security Auckland University of Technology].

Musoni, M., Domingo, E., & Ogah, E. (2023). Digital ID systems in Africa: Challenges, risks and opportunities. In: ECDPM Discussion Paper 360. Maastricht: ECDPM.

Mysore, I. (2023). Role of Digital Identity in Advancing Global Health: A 360 Perspective. In Digital Identity in the New Era of Personalized Medicine (pp. 1-27). IGI Global.

Naz, I., & Khan, S. N. (2024). Impact of forensic accounting on fraud detection and prevention: a case of firms in Pakistan. Journal of Financial Crime.

Ng, J. K. C. (2025). Digital Identity in Fintech Regulation: Explores the Role of Regulation on Digital ID in the Fintech Industry. In Examining Global Regulations During the Rise of Fintech (pp. 335-370). IGI Global Scientific Publishing.

Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). Harnessing Artificial Intelligence and Machine Learning for Fraud Detection and Prevention in Nigeria. Journal of Economic Criminology, 100127.

Oduri, S. (2024). Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era. International Journal of Innovative Research in Science Engineering and Technology, 13(7), 13632-13640.

Oguta, G. C. (2024). Securing the virtual marketplace: Navigating the landscape of security and privacy challenges in E-Commerce. GSC Advanced Research and Reviews, 18(1), 084-117.

Olomukoro, C. (2023). The effects of implementing blockchain technology in the central bank of nigeria. A PhD Thesis Dissertation Manuscript, Unicaf University, Malawi.

Onwubiko, C. (2020). Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. Computers & Security, 96, 101900.

Ray, B., Ghosh, S., Ahmed, S., Sarkar, R., & Nasipuri, M. (2022). Outlier detection using an ensemble of clustering algorithms. Multimedia Tools and Applications, 81(2), 2681-2709.

Reurink, A. (2018). Finance crime. In Oxford Research Encyclopedia of Criminology and Criminal Justice.

Schardong, F., & Custódio, R. (2022). Self-sovereign identity: a systematic review, mapping and taxonomy. Sensors, 22(15), 5641.

Volume 5 Issue No 1 (2026)
Online ISSN: 3006-2047
Print ISSN: 3006-2039

Senecal, D. (2024). The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet. John Wiley & Sons.

Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Mashat, A., Kumar, A., & Kumar, M. (2022). Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison. Mobile Information Systems, 2022(1), 8930472.

Soltani, R., Nguyen, U. T., & An, A. (2021). A Survey of Self-Sovereign Identity Ecosystem. Security and Communication Networks, 2021(1), 8873429.

Štitilis, D., Laurinaitis, M., & Verenius, E. (2023). The Use of biometric technologies in ensuring critical infrastructure security: the context of protecting personal data. Entrepreneurship and sustainability issues, 10(3), 133.

Theodorakopoulos, L., Theodoropoulou, A., & Stamatiou, Y. (2024). A state-of-the-art review in big data management engineering: Real-life case studies, challenges, and future research directions. Eng, 5(3), 1266-1297.

Tiham, F. M., Fahim, A. R., Julcarnine, G. M., & Usman, H. M. (2024). Decentralized identity verification: a blockchain-based framework for self-sovereign identity (SSI) with issuer trust registry Brac University].

Verma, B., Singla, B., & Mittal, A. (2024). Digital Technologies, Ethics, and Decentralization in the Digital Era. IGI Global.

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. Frontiers in Blockchain, 2, 28.

Wang, M., Fu, W., He, X., Hao, S., & Wu, X. (2020). A survey on large-scale machine learning. IEEE Transactions on Knowledge and Data Engineering, 34(6), 2574-2594.

Wewege, L. (2017). The digital banking revolution. Lulu. com.

Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: a review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. Applied Sciences, 14(2), 675.

Yadav, S. (2024). Decentralizing Identity with Blockchain Technology in Digital Identity Management. Journal of Current Research in Blockchain, 1(3), 178-189.

Yarovenko, H., & Rogkova, M. (2022). Dynamic and bibliometric analysis of terms identifying the combating financial and cyber fraud system. Financial Markets, Institutions and Risks (FMIR), 6(3), 93-104.

Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: universal identity management and the concept of the “Self-Sovereign” individual. Frontiers in Blockchain, 3, 26.