2025 Volume: 01 Issue: 05 www.ijrpa.com Review Article

International Journal Research Publication Analysis

Page: 312-323

AI APPLICATIONS FOR E-KYC AND IDENTITY FRAUD DETECTION IN BANGLADESH'S FINTECH SECTOR: A LITERATURE REVIEW

Sujit Kumar Sarker*

Senior Engineer (IT), Sonali Bank PLC., Dhaka, Bangladesh.

Article Received: 08 August 2025
Article Revised: 28 August 2025
Published on: 18 September 2025

***Corresponding Author: Sujit Kumar Sarker**
Senior Engineer (IT), Sonali Bank PLC., Dhaka, Bangladesh.
Email ID: sksarker.ru@gmail.com,

ABSTRACT

The astounding development of FinTech in Bangladesh has substantially elevated the usage of the digital financial product ecosystem in banking, mobile financial services (MFS) like Bkash, Nagad, Rocket, Upay, etc., online transactions, etc., as well as financial transactions via e-commerce such as Pickaboo, Othoba, Daraz, etc., m-commerce such as Mobile apps, Bangla QR code, etc. This burgeoning trend has, however, left the e-financial ecosystem vulnerable to identity fraud, phishing, spoofing, social engineering, and other fraudulent complaints. The ever-changing nature of fraud makes traditional rule-based fraud detection ineffective. However, AI- powered fraud detection techniques such as machine learning, deep learning, behavioral profiles, federated learning, etc. have been shown to strengthen e-KYC and fraud detection. This article provides a systematic literature review of AI in e-KYC and fraud Detection in the context of the FinTech ecosystem in Bangladesh. It also discusses the existing literature, highlights the gaps and exigent areas for further research.

KEYWORDS: FinTech, Bangladesh, e-KYC, Identity Fraud, Fraud Detection, Spoofing, Social Engineering, Mobile Financial Services (MFS), e-commerce, m-commerce Artificial Intelligence (AI), Machine Learning, Federated Learning, Explainable AI (XAI), Financial Inclusion.

1. INTRODUCTION AND BACKGROUND

The literature review of earlier studies on AI applications for e-KYC and identity fraud detection in the FinTech sector in Bangladesh has been conducted to identify existing gaps and inconsistencies in the effectiveness of the systems to prevent fraud.

Interestingly, the available literature and studies reflect that there are some generic similarities that come across many studies. It appears that, in most cases, the studies conducted various investigations into the aspects of fraud detection methodologies in the FinTech sector, and those investigations came up with strong evidence.

According to (West et al., 2015), financial fraud schemes persist across industries, highlighting the insufficient capabilities of contemporary manual detection controls in identifying complex schemes. The paper stated that computational intelligence and data mining can effectively model small variations in data using large data samples. Financial fraud schemes evolve alongside technological improvements and exploit new vulnerabilities, emphasizing the need for precise, timely, and automated detection methodologies to adapt to fraud nature changes.

Continuing from this, (Ahmed Soomro et al., 2019) investigated identity fraud handling in e-tail. The study stated that there is an overall lack of literature that is grounded by theory other than deterrence theories, and there is little contextually specific literature. Based on the systematic literature review, the study grounded common acceptance within the literature around illustrative fraud handling methods designed to manipulate the dimensions of authentication, information security, corrective action, attribute posting, transaction mediation, transaction deterrence, system hacking as well as customer communication. However, there is an absence of literature examining and grounding fraud handling methods of e-tail organizations on the boundaries of counter-acceptance, counter-affiliation, counter-involvement, counter-posting, and customer ledger manipulation, which was regarded as extremely important. The study goes on to state that since deception is a remarkable element of the e-tail environment, fraud counteractions and mitigation on the basis of real-time and retrospective fraud handling are critical. In order to mitigate risks after deception acceptance and engagement, customers need to frequently update their transactions and biography ledgers. Thus “constancy” and “proactivity” are essential fraud handling techniques.

Furthering this in another stream, in response to the decade-long rise of online banking and the new fraud dynamics it has created, (Mehana & Pireva Nuci, 2020) proposed a data-driven anti-fraud approach. The study stated that fraud detection is based on an adaptive anti-fraud detection architecture and incremental classifier that enables real-time identification of ongoing fraud incidents with an industry-leading fraud

detection rate. Embedded systems require specialized change detection methods to increase the degree of adaptability in the model parameters, which represents the skeleton of the incremental classifier. The proposed architecture allows for significant scalability and flexibility, particularly during situations of abrupt changes in transaction behavior or fraud tactics. It was stated that this research leads to the inference that timely fraud detection is straightforward and easy to implement with an out-of-the-box solution when incremental modeling is applied.

Next, (Elliott et al., 2021) explored the tensions between innovators and regulators in financially inclusive innovations that require the deployment of privacy-sensitive technologies for authenticating clients and transacting on their behalf. The study used qualitative semi-structured interviews with innovators and regulators to explore the deployment of decentralized identifiers and verifiable credentials, an emerging digital identity technology. The findings indicate that regulators' risk-based approach to service innovation is challenged by the environment of pushback and adaptation required for legacy services to stay relevant and tiered services for vulnerable groups to be effective. Drawn from the analysis, the paper identifies three tensions that stem from ambiguously scalable elements of decentralized identifiers and verifiable credentials. The paper discusses how these tensions result from value perceptions and activist dynamics between innovators and regulators and the implications for innovating with techno-social systems in risk context.

Lastly, (Awosika et al., 2023) noted the trend of financial fraud as a result of the emergence of online banking and the specific fraudulent techniques utilized by bank account fraud. The authors argued that Machine Learning and Federated Learning models should be utilized and combined to detect fraudulent activities. Focus was made on Explainable AI (XAI) where the study mentioned that it deals with how and why decisions made by Artificial Intelligence (AI) systems can be understood due to their opaqueness. User trust in such systems increases with transparency of the decision-making process behind their recommendations. The paper discussed that one way to explain the AI model's decision-making process is to quantify the contributions of various input features to a specific outcome or prediction. Therefore, model training over multiple devices rather than on centralized cloud servers was proposed. In such decentralized frameworks, user devices retain data locally to train models. The model improvements and updates are then shared with the central server, ensuring that

sensitive data does not leave users' devices. The paper proposed a collaborative fraud detection framework that incorporates user-level transparency by integrating XAI into Federated Learning for financial institutions.

Based on these articles, it can be concluded that the literature review of past studies on AI applications in e-KYC and identity fraud detection in the FinTech sector in Bangladesh investigates the effectiveness of the current methodologies in practice while identifying potential gaps in the literature that would require further study and investigation in the future.

2. METHODOLOGY

The methodology of this study is a qualitative systematic literature review. It aims at providing a better understanding of AI-powered e-KYC-based identity fraud detection by synthesizing the available knowledge and identifying its themes, issues, advancements, research gaps, and potential implications for Bangladesh.

2.1. Research Design

The research design is non-empirical and analytical, involving a systematic examination, collection, and critical analysis of existing literature, published data, and scholarly contributions such as journal articles, conference papers, websites, online articles, reports, gray literature, academic thesis works, and industry papers.

2.2. Data Collection (Literature Search)

A systematic literature search was performed on Google Scholar, IEEE Xplore, Scopus, and SpringerLink. The query string utilized combinations of the following keywords and Boolean logic:

"AI-powered e-KYC" OR "AI applications in e-KYC"

"AI identity verification" OR "AI applications in identity verification" "Digital identity fraud detection" AND "machine learning"

"FinTech" AND "Bangladesh"

"fraud" AND "Spoofing", AND "Social Engineering"

"Mobile Financial Services (MFS)" AND "e-commerce" AND "m-commerce" "Federated Learning financial fraud"

"Explainable AI" AND "KYC"

Limiting the search scope, only literature published between 2015 and 2023 is included in this study to ensure the topicality of technological paradigms.

2.3. Data Analysis

Thematic analysis was used to analyze literature. The phases of thematic analysis precede distinct research phases and consist of:

Familiarization: The first phase involves the researcher immersing themselves in the data set, reading and rereading the articles to become deeply familiar with its content.

Coding: During this phase, features of the data relevant to the research questions are identified, and data sets are collated analytically. Initial codes are created for each source, including the article's main argument, findings, and any specific difficulties encountered.

Theme development: The next step involves collating codes to form broader analytical themes that encompass all relevant data. Key themes derived from the analysis included:

- Limitations of traditional fraud detection approaches.
- Strengths of adaptive data-driven AI algorithms over rule-based static systems.
- Few developing nations' context-specific research.
- Innovation versus compliance dilemma.
- Privacy (achieved throughtechniques like Federated Learning) and transparency (facilitated by Explainable AI approaches).

2.4. Limitations

The study inherently suffers from limitations imposed by the number and nature of available academic sources and the quality of existing research in this domain. A particular limitation of the study is the number of publications addressing the applicability of AI-based e-KYC to combat identity fraud published in the context of Bangladesh's FinTech ecosystem. Since there are only a limited number of published studies, insights from a few international studies have been used to highlight and extrapolate the key issues. The application of secondary data sets as a practice- oriented qualitative methodology signals a significant gap to be filled by future primary data researcher endeavors.

3. REVIEW OF LITERATURE

The article "Intelligent Financial Fraud Detection Practices: An Investigation" by West, Bhattacharya, and Islam (2015) offers a comprehensive examination of the challenges and technological solutions associated with detecting financial fraud in contemporary

settings. The authors emphasize that financial fraud presents substantial risks to various stakeholders, including financial institutions, governments, and consumers, particularly as reliance on cloud computing and mobile technologies increases (West et al., 2015). This context underscores the necessity for advanced detection mechanisms capable of addressing the evolving sophistication of fraudulent activities.

A critical contribution of the article is its critique of traditional manual detection methods, such as auditing, which are deemed inefficient and unreliable amid the proliferation of big data. The authors advocate for the adoption of automated techniques, specifically data mining and computational intelligence, which are better suited to identify minute anomalies within vast datasets. This shift from manual to automated detection aligns with the broader trend toward leveraging artificial intelligence and machine learning in financial fraud detection, a pertinent consideration for AI-powered e-KYC systems in Bangladesh's fintech landscape.

Furthermore, the article delineates the complexity of financial fraud, noting that it encompasses several types that demand tailored detection strategies. The authors highlight how advancements in internet and mobile technologies have facilitated the rise of sophisticated fraud schemes, compelling financial institutions to continuously evolve their detection approaches. This insight is particularly relevant when considering the integration of AI-driven fraud detection within e-KYC frameworks, as it underscores the importance of adaptable and intelligent systems capable of countering increasingly complex fraudulent tactics.

However, the article primarily concentrates on the technical aspects of fraud detection within the financial sector without explicitly addressing the specific challenges faced by developing countries like Bangladesh. While its discussion on the effectiveness of data mining and computational intelligence provides valuable guidance, it lacks a detailed exploration of contextual factors such as infrastructure limitations, regulatory environments, and user acceptance that are critical for implementing AI applications in e-KYC solutions in Bangladesh.

The article "Investigating Identity Fraud Management Practices in E-tail sector: A Systematic Review" by Soomro et al. (Ahmed Soomro et al., 2019) offers a comprehensive overview of the existing literature concerning identity fraud management, primarily emphasizing information security and authentication

mechanisms. The authors highlight a significant research gap in the context of e-tail organizations, noting that most studies are rooted in fear appeal and general deterrence theories, with limited focus on the specific operational challenges faced by online retail sectors.

A critical evaluation reveals that while the article effectively consolidates the predominant themes in fraud prevention such as biometric technologies, behavioral analysis, and real-time detection systems, it also underscores the paucity of research dedicated to e-tail-specific policies, communication strategies, and organizational compliance. This gap is particularly pertinent given the rapid digital transformation within Bangladesh's FinTech landscape, where tailored fraud detection and identity verification solutions are essential for safeguarding customer data and maintaining trust. Furthermore, the emphasis on technical measures, like auto-detection systems and regular customer record updates, aligns with current best practices in information security. However, the article points out that there is comparatively less focus on policy development and awareness initiatives, which are crucial components for a holistic approach to identity fraud mitigation. This oversight suggests that future research should integrate policy frameworks with technological solutions to enhance the effectiveness of fraud management in e-tail environments.

The article "Fraud Detection using Data-Driven approach" by Mehana and Nuci (Mehana & Pireva Nuci, 2020) provides a comprehensive examination of the challenges and solutions associated with online fraud detection, particularly within the context of internet banking. The authors highlight that the proliferation of internet banking, which began with the introduction of online banking services in 1980 by United American Bank, has significantly increased both convenience for users and the complexity of data management. This evolution has, however, been accompanied by a rise in fraudulent activities, necessitating advanced detection mechanisms.

A critical contribution to this work is the emphasis on real-time, adaptive fraud detection models capable of addressing the dynamic and rapidly evolving nature of online financial transactions. The authors propose an incremental classifier that operates continuously, filtering fraudulent behavior as it occurs, which is particularly relevant for AI-powered e-KYC systems aiming to prevent identity fraud in Bangladesh's FinTech sector. The model's ability to identify anomalies with up to 97% accuracy demonstrates

its effectiveness, while its low operational costs make it a practical solution for large-scale deployment.

However, the article also underscores the challenges posed by the vast and complex data generated in online banking environments. The high volume and velocity of data demand robust, scalable algorithms that can adapt to new fraud patterns without significant delays. While the incremental classifier approach shows promise, the article does not delve deeply into potential limitations such as false positives, model drift over time, or the need for continuous data labeling and model retraining, which are critical factors in real-world applications.

The article titled "Know Your Customer: Balancing Innovation and Regulation for Financial Inclusion" offers a comprehensive examination of the delicate balance between technological innovation and regulatory compliance in the context of financial inclusion. It emphasizes the importance of designing services that accommodate vulnerable populations while adhering to strict regulatory frameworks, a challenge particularly relevant to AI applications in e-KYC and identity fraud detection systems in Bangladesh's FinTech sector.

The authors explore the inherent tension between privacy-preserving, adaptive service provision and regulatory requirements through a qualitative analysis involving banking experts. This approach provides valuable insights into the practical considerations and constraints faced by financial institutions when deploying digital identity solutions (Elliott et al., 2021). A key contribution of the article is the demonstration of a prototype utilizing open-source decentralized identifiers (DIDs) and verifiable credentials, technologies that enable selective disclosure. This approach aligns with the needs of AI-powered e-KYC systems by allowing individuals to control their sensitive information, thereby enhancing privacy and reducing identity fraud risks.

Critically, the article underscores the potential of digital identity technologies to facilitate financial inclusion, especially among vulnerable populations often excluded from traditional banking services. The prototype exemplifies how such technologies can be integrated into existing regulatory frameworks to strike a balance between security, privacy, and accessibility. However, while the technological promise is evident, the article also highlights the challenges of implementation, including regulatory acceptance, technological literacy, and infrastructure readiness—factors that are

particularly pertinent to Bangladesh's rapidly evolving FinTech landscape.

The article by Awosika, Shukla, and Pranggono provides a comprehensive examination of how emerging AI techniques can bolster fraud detection mechanisms within the financial sector, with relevance to Bangladesh's FinTech landscape. Central to their discussion is the integration of Federated Learning (FL) and Explainable AI (XAI), which collectively address critical challenges faced by traditional machine learning models in fraud detection, such as data privacy concerns and lack of transparency.

The authors articulate that bank account fraud, including unauthorized transfers and identity theft, poses significant threats to financial security, necessitating sophisticated detection systems. They highlight that conventional ML approaches often struggle with data imbalance and the heterogeneity of fraudulent activities across institutions. FL emerges as a promising solution by enabling collaborative model training across multiple banks without the need for direct data sharing, thereby preserving privacy, a vital consideration in the context of Bangladesh's sensitive financial data (Awosika et al., 2023). This decentralized approach not only mitigates privacy concerns but also enhances the robustness of fraud detection models through diverse data inputs.

Furthermore, the article emphasizes the importance of XAI in making AI-driven decisions interpretable and trustworthy. By providing transparent insights into the model's reasoning, XAI can foster greater confidence among stakeholders and facilitate regulatory compliance, which is especially pertinent in Bangladesh's evolving regulatory environment. The proposed hybrid model combining FL and XAI exemplifies a strategic advancement in creating privacy-preserving, collaborative, and transparent fraud detection systems.

Critically, while the article convincingly advocates for the integration of FL and XAI, it could benefit from a more detailed discussion on the practical implementation challenges, such as computational overhead, model convergence issues, and the need for standardized protocols across diverse banking institutions. Nonetheless, the insights presented are highly relevant for developing AI-based in e-KYC and identity fraud detection solutions in Bangladesh, emphasizing the importance of balancing privacy, collaboration, and transparency in financial AI applications.

4. DISCUSSION AND FINDINGS

The overarching findings of this literature review are multifaceted and aligned with the research goal of identifying best practices for AI applications in e-KYC and identity fraud detection in Bangladesh's FinTech industry. Firstly, there is a clear consensus across studies about the inadequacy of current manual and rule-based systems for detecting fraudulent activity (West et al., 2015) and the necessity for these systems to be automated and adaptable. The need for a robust and adaptable real-time automated detector could also protect those financial institutions that feel the data risk is worth it from the dynamic, sophisticated nature of financial fraud, as implied by the 97% detection rate of Mehana and Nuci's (2020) incremental classifier. However, effectiveness is not enough. As pointed out by Soomro et al. (2019) about the existence of a research gap, this discussion cannot be generalized. The solution for Bangladesh is not simply the adoption of technology or adequate empowerment of industries, as Allam (2020) claimed. These technologies must be adapted to the specific operational contexts, human behaviors, and data infrastructures of Bangladesh. The literature discussion also benefits from the important tension between innovation and regulation highlighted in Elliott et al. (2021) through their discussion of Decentralized Identifiers (DIDs) as a privacy-enhancing technology. Framed alongside Geva's (2021) call to strive for increased financial participation and inclusiveness in the Bangladeshi context, this further directs the discussion toward best practices that could first and foremost be regulatory compliant. The importance of explainable and transparent systems can also be deduced from literature to achieve this regulatory goal. The literature highlights an increasing call for the integration of Federated Learning (FL) and Explainable AI (XAI) in fraud detection systems, as discussed by Awosika et al. (2023). FL, as a federated machine learning approach, preserves data interrogation by allowing banks and financial institutions to collaboratively train an AI model without sharing sensitive training data. This could solve the problem of data silos, but as mentioned, it does not replace the need for adequate interpretability. The "black box" problem of AI must still be addressed to build trust between customers and financial institutions, as mandated by regulation in many jurisdictions. Here, an XAI model can guide decision-makers toward a model- friendly understanding of the AI to create explainability and, thus, trust. This leads us to the conclusion that, overall and primarily, Bangladesh must look to a framework that is real-time and effective, adaptable and innovative, regulatorily compliant, privacy-preserving, and transparent to achieve

sustainable financial inclusion in the industry.

5. CONCLUSION

The literature on AI applications in e-KYC and identity fraud detection within Bangladesh's FinTech sector reveals a complex interplay between technological advancements and the pressing need for effective fraud prevention strategies. The reviewed studies collectively underscore the inadequacies of traditional detection methods and highlight the transformative potential of AI and machine learning technologies in enhancing fraud detection mechanisms.

The article by West, Bhattacharya, and Islam (West et al., 2015) emphasizes the limitations of manual detection methods in the face of evolving financial fraud, advocating for automated techniques such as data mining and computational intelligence to identify anomalies within large datasets. This perspective aligns with the increasing reliance on AI-driven solutions, which are essential for adapting to the sophisticated nature of fraud in the digital age.

Soomro et al. (Ahmed Soomro et al., 2019) further contribute to this discourse by identifying a significant gap in research focused on identity fraud management practices specifically tailored for e-tail organizations. Their systematic review highlights the need for real-time mitigation strategies and the importance of regularly updating customer records, suggesting that a more contextual approach is necessary for effective fraud management.

Mehana and Nuci (Mehana & Pireva Nuci, 2020) introduce a data-driven approach that employs an incremental classifier for real-time fraud detection in online banking, achieving high accuracy rates. Their findings reinforce the necessity for adaptive models that can respond to the rapid changes in online financial transactions, emphasizing the critical role such innovations play in AI-powered e-KYC systems.

The qualitative study by Awosika, Shukla, and Pranggono (Awosika et al., 2023) explores the intersection of innovation and regulation, advocating for privacy- sensitive technologies like decentralized identifiers and verifiable credentials. Their insights reveal the potential of these technologies to enhance financial inclusion while addressing privacy concerns, an essential consideration for developing effective fraud detection systems.

Lastly, the article by Awosika et al. (Elliott et al., 2021) delves into the integration of Federated Learning and Explainable AI, proposing a collaborative framework that preserves user privacy and fosters trust among stakeholders. This approach highlights the importance of transparency and collaboration in developing robust fraud detection systems tailored to the unique challenges faced within Bangladesh's FinTech landscape.

In conclusion, the literature collectively underscores the urgent need for advanced, context-specific fraud detection mechanisms in Bangladesh's FinTech sector. The integration of AI, machine learning, and innovative technologies can significantly enhance e-KYC processes and identity fraud detection. However, future research must also address practical implementation challenges, regulatory compliance, and the need for continuous adaptation to evolving fraud tactics.

REFERENCES

1. West, J., Bhattacharya, M., & Islam, R. (2015). Intelligent Financial Fraud Detection Practices: An Investigation. [https://arxiv.org/pdf/1510.07165]
2. Ahmed Soomro, Z., Ahmed, J., Hussain Shah, M., & Khoumbati, K. (2019). Investigating Identity Fraud Management Practices in E-tail sector: A Systematic Review. [https://core.ac.uk/reader/169432910.pdf]
3. Mehana, A. & Pireva Nuci, K. (2020). Fraud Detection using Data-Driven approach. [https://arxiv.org/pdf/2009.06365]
4. Elliott, K., Coopamootoo, K., Curran, E., Ezhilchelvan, P., Finnigan, S., Horsfall, D., Ma, Z., Ng, M., Spiliotopoulos, T., Wu, H., & van Moorsel, A. (2021). Know Your Customer: Balancing Innovation and Regulation for Financial Inclusion. [https://arxiv.org/pdf/2112.09767]
5. Awosika, T., Mani Shukla, R., & Pranggono, B. (2023). Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection. [https://arxiv.org/pdf/2312.13334]