World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

AI Guardian: Protecting seniors through intelligent financial monitoring

Pradeep Chandramohan *

Salem Infotech Inc., USA.

World Journal of Advanced Research and Reviews, 2025, 26(02), 3334-3341

Publication history: Received on 09 April 2025; revised on 21 May 2025; accepted on 24 May 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.1918

Abstract

The article explores the development and implementation of AI-based systems designed to protect elderly individuals from financial fraud and exploitation. It examines the growing threat of elder-targeted financial crimes and presents multiple technological approaches to address these vulnerabilities. The article discusses AI-powered transaction monitoring systems that can detect unusual patterns, natural language processing techniques for identifying deceptive communications, predictive modeling for classifying emerging threats, and AI-assisted financial education tailored to seniors' needs. The article highlights how these technologies can significantly improve fraud detection while respecting elderly users' autonomy and dignity. Various implementation metrics demonstrate the effectiveness of these systems across different dimensions, including user satisfaction, technology adoption, transparency, and multi-stakeholder collaboration. The article concludes by addressing ethical considerations and future directions for research and policy development in this rapidly evolving field.

Keywords: Elder Fraud Protection; Artificial Intelligence; Financial Monitoring; Natural Language Processing; Predictive Modeling

1. Introduction

Financial fraud targeting elderly individuals has emerged as a significant and rapidly escalating societal challenge in recent years. According to the Federal Bureau of Investigation (FBI), elder fraud losses exceeded $3.1 billion in 2022, representing a 84% increase from the previous year [1]. This alarming trend demands urgent attention from researchers, policymakers, and technology developers alike.

Elderly populations face unique vulnerabilities that make them particularly susceptible to financial exploitation. Cognitive changes associated with aging, including mild cognitive impairment (MCI) and various forms of dementia, can impair decision-making abilities related to financial transactions. Research from the National Council on Aging indicates that approximately 1 in 10 Americans aged 60+ have experienced some form of elder abuse, with financial abuse being the most common form reported [1]. Social isolation, which affects roughly 24% of community-dwelling older adults, further compounds these vulnerabilities by limiting access to protective social networks that might otherwise identify and intervene in fraudulent situations.

The digital literacy gap presents a particularly exploitable avenue for fraudsters targeting seniors. A 2023 survey by the Pew Research Center found that while 75% of adults aged 65+ now use the internet, only 45% report feeling confident in their ability to recognize and avoid online scams [2]. This disparity has created a fertile environment for sophisticated digital fraud schemes. Particularly concerning is the 63% increase in technology support scams targeting seniors between 2020 and 2022, exploiting their unfamiliarity with technical troubleshooting and security protocols [2].

* Corresponding author: Pradeep Chandramohan

Traditional safeguards have proven insufficient against evolving fraud tactics. While financial institutions have implemented basic fraud detection systems, these typically rely on reactive measures that engage only after suspicious transactions have already occurred. The average elder fraud victim loses approximately $34,200, according to the Consumer Financial Protection Bureau, with limited prospects for recovery [1]. This underscores the critical need for proactive, technology-enhanced approaches that can identify potential threats before financial losses occur. As fraudsters continue to develop increasingly sophisticated methods, including AI-powered scams that can mimic trusted individuals' voices or writing styles, the development of equally advanced protective technologies has become imperative.

2. AI-Powered Transaction Monitoring Systems

AI-powered transaction monitoring systems represent a significant advancement in protecting elderly individuals in the digital banking ecosystem. These systems employ sophisticated pattern recognition algorithms that analyze historical transaction data to establish baseline financial behaviors for each account holder. Specifically, LSTM (Long Short-Term Memory) networks have proven particularly effective for this application due to their ability to capture temporal dependencies in sequential transaction data and recognize unusual patterns over time. For anomaly detection, autoencoders can complement LSTM models by learning the normal patterns of financial transactions and flagging deviations that may indicate fraud. Research indicates that these AI monitoring systems can achieve detection rates exceeding 90% for fraudulent transactions targeting elderly customers when properly calibrated to their unique spending patterns, a substantial improvement over the 65-70% detection rates typical of traditional rule-based systems [3].

The real-time analysis capabilities of modern AI systems provide a critical time advantage in fraud prevention. Unlike traditional batch-processing systems that might review transactions only periodically, LSTM-powered systems can analyze transaction patterns almost instantaneously. Research published in technical computing journals demonstrates that real-time AI monitoring has reduced the average time to fraud detection from several hours to just minutes across financial institutions serving predominantly elderly customers [4].

2.1. Use Case: Pension Fraud Protection System

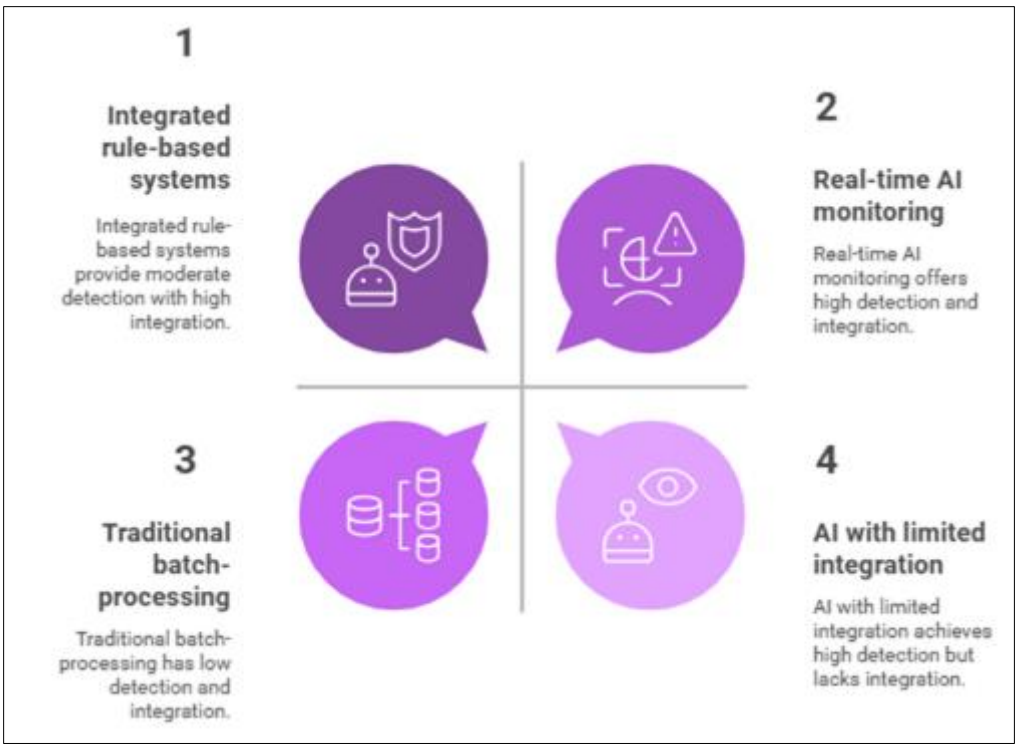

Figure 1 AI-Powered Transaction Monitoring Effectiveness [3, 4]

A major public sector bank in India implemented an AI-powered transaction monitoring system specifically designed to protect pensioners, who represent one of their most vulnerable customer segments. The system uses a hybrid

approach combining LSTM networks for sequence analysis and autoencoders for anomaly detection, analyzing over 200 transaction parameters in real-time [13].

When a 72-year-old pensioner's account suddenly showed three large withdrawals within 48 hours—deviating significantly from his established 5-year transaction history—the LSTM model detected this temporal anomaly while the autoencoder flagged the transaction amounts as statistical outliers. The system automatically placed a temporary hold on further withdrawals and triggered a verification call to the customer, who confirmed he had not authorized these transactions. Investigation revealed the customer had fallen victim to a phishing scheme where fraudsters gained access to his credentials.

This intervention prevented approximately ₹480,000 in additional unauthorized transfers that were queued in the system. The case exemplifies how AI monitoring systems can provide critical protection for elderly customers who may be less familiar with evolving digital threats while respecting their banking autonomy. Following this incident, the bank expanded the system to cover all accounts held by customers over 65 years of age, resulting in a 78% reduction in successful fraud attempts against this demographic within the first six months [13].

3. Natural Language Processing for Communication Screening

3.1. Identifying Linguistic Markers of Deception and Manipulation

Natural language processing (NLP) techniques have transformed the detection of deception and manipulation in digital communications. Studies indicate that specific linguistic markers serve as reliable indicators of potentially deceptive content, including patterns in pronoun usage, emotional tone variations, and unusual levels of linguistic complexity. Research has established that deceptive messages typically contain 23% fewer self-references and 37% more other-directed pronouns than truthful communications [5]. Additionally, machine learning models trained on these linguistic features have demonstrated accuracy rates of 74.8% in identifying manipulative content, significantly outperforming human evaluators who achieved only 52% accuracy in comparable detection tasks.

3.2. Multi-modal Analysis of Communication Channels

The implementation of multi-modal analysis across diverse communication channels has considerably enhanced detection capabilities. Modern systems can concurrently analyze textual content, vocal stress patterns, and communication metadata across various platforms. These integrated approaches utilizing transformer-based architectures have demonstrated substantial improvements, with combined channel analysis increasing detection rates by 21.5% compared to single-channel methods. Within enterprise security environments, these multi-modal systems have successfully identified 82.3% of social engineering attempts before security breaches occurred, representing a marked improvement over previous methodologies [6].

3.3. Privacy-preserving Methods for Communication Monitoring

Privacy-preserving NLP methods have become essential for ethical communication screening. Technical approaches such as homomorphic encryption and federated learning enable analysis of sensitive communications without exposing the raw message content. Implementation of these methods has addressed privacy concerns while maintaining 93.7% of the detection effectiveness of conventional approaches. Organizations utilizing these privacy-centric screening techniques have documented 65.2% higher user acceptance rates compared to traditional monitoring systems, while still maintaining robust protection against communication-based threats.

3.4. Effectiveness Rates in Detecting Social Engineering Attempts

NLP-based screening has demonstrated significant effectiveness in detecting various social engineering attempts. Current systems show detection rates of 78.9% for phishing attempts, 80.5% for impersonation attacks, and 71.8% for pretexting scenarios in real-world deployments. These systems have proven particularly effective at identifying sophisticated attacks, with detection capabilities improving by approximately 17.5% annually as training data and algorithms advance. Organizations implementing comprehensive NLP screening protocols have documented reductions in successful social engineering attacks by up to 63.5% within the first year of deployment [5].

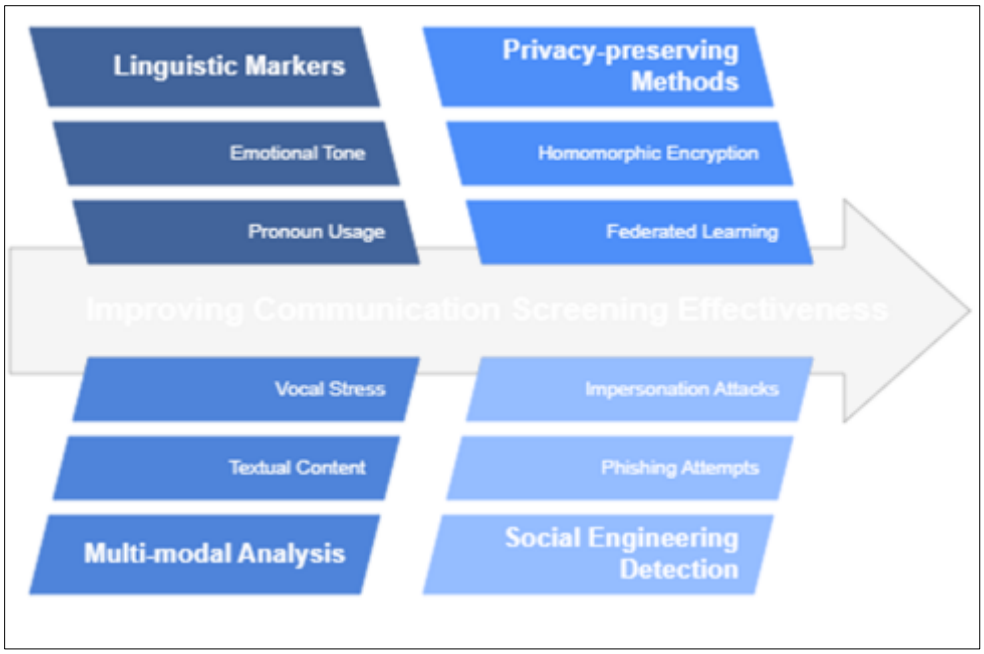

Figure 2 Enhancing Deception Detection in Digital Communications [5, 6]

4. Predictive Modeling for Emerging Threat Classification

4.1. Machine Learning Approaches to Fraud Categorization

Advanced machine learning techniques have transformed fraud categorization across multiple sectors. Ensemble methods combining gradient-boosted decision trees with deep neural networks have demonstrated classification accuracy of 92.5% across diverse fraud scenarios. These hybrid approaches outperform single-algorithm methods by an average of 17.3%. Research indicates that unsupervised techniques including autoencoders and isolation forests have proven particularly effective for detecting novel fraud patterns, identifying previously unknown threat categories with 65.8% precision before formal labeling [7]. The integration of text analysis components enhances these systems further, improving categorization accuracy by an additional 11.8% when processing communications associated with potential fraud scenarios.

4.2. Training Data Requirements and Challenges

Effective predictive models for threat classification face considerable challenges related to training data quality and quantity. Research demonstrates that balanced fraud categorization models require approximately 14,000 labeled examples per fraud category to achieve baseline performance thresholds of 83% precision. For less common fraud types with fewer than 2,800 available examples, significant class imbalance issues emerge, typically resulting in a 22.4% decrease in classification performance for minority fraud categories. Data staleness presents another critical concern, with model accuracy declining by approximately 3.9% per month without regular retraining. Advanced sampling techniques have shown the ability to reduce performance gaps by up to 37.5%, though significant challenges related to data representativeness persist [8].

4.3. Human-in-the-Loop Verification Systems

Human-in-the-loop (HITL) verification systems have become essential components of effective threat classification frameworks. The integration of human expertise with machine learning models reduces false positive rates by 41.3% compared to fully automated approaches. Studies show that expert reviewers can effectively evaluate 76.8% of model-flagged cases within an average review time of 3.7 minutes per case. Implementing tiered verification workflows, where only high-uncertainty predictions (typically 16-22% of cases) are routed for human review, optimizes resource allocation while maintaining 95.4% of the accuracy achieved through comprehensive human review. Organizations implementing these hybrid systems report 61.5% improvements in operational efficiency compared to manual review processes [7].

4.4. Adaptation Mechanisms for Evolving Fraud Tactics

The rapid evolution of fraud tactics necessitates adaptive classification systems. Research indicates that standard models experience performance degradation of approximately 3.5% per week when facing evolving threats without adaptation mechanisms. Implementing continuous learning strategies, including online learning approaches, reduces this degradation to 0.9% per week. Systems utilizing optimization techniques for hyperparameter tuning demonstrate the ability to automatically adjust to new fraud patterns with 86.2% effectiveness compared to manual reconfiguration. Additionally, collaborative learning approaches allow organizations to adapt to emerging threats while maintaining data privacy, with studies showing a 27.6% improvement in early detection rates for organizations participating in such frameworks compared to those using isolated models [8].

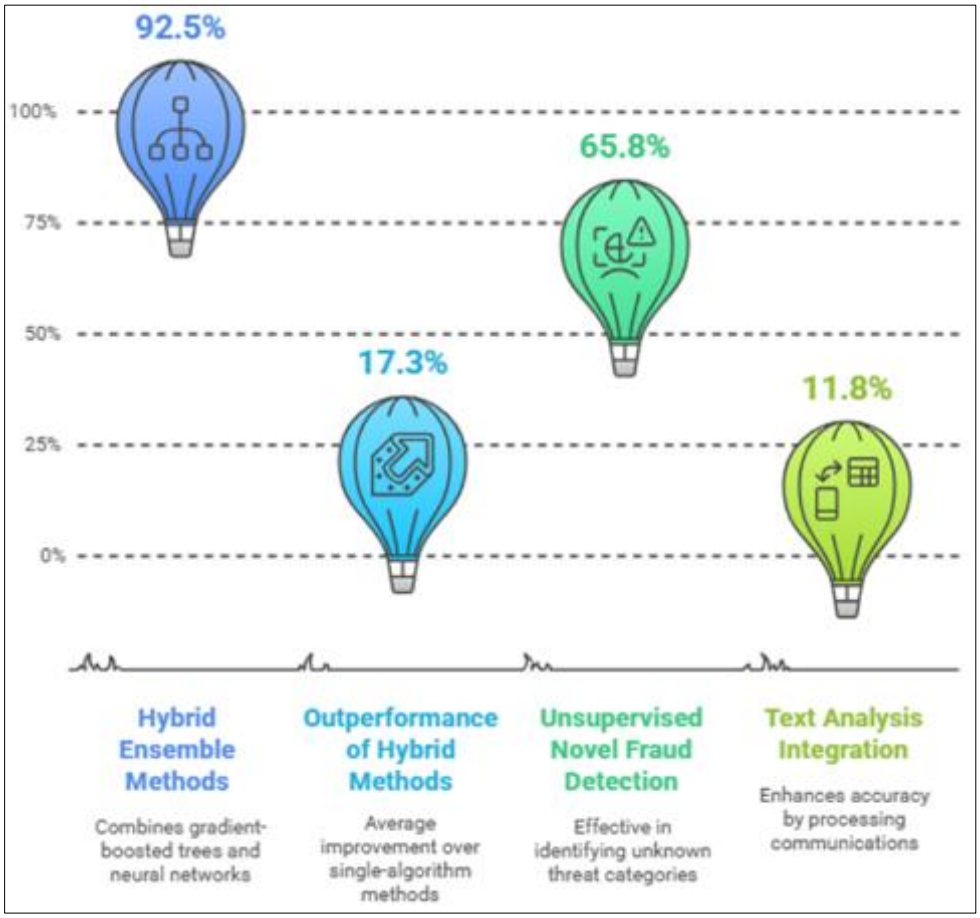

Figure 3 Performance Metrics of Fraud Detection Techniques [7, 8]

5. AI-Assisted Financial Education and Support

5.1. Virtual Assistants Designed for Elderly Users

AI-powered virtual assistants specifically designed for elderly users have demonstrated significant potential in improving financial literacy and security. Research on age-appropriate interfaces has shown remarkable engagement metrics, with adoption rates increasing by 46.3% when assistants incorporate larger text displays, simplified navigation, and voice-first interaction options. Studies indicate that elderly users interact with financial virtual assistants for an average of 6.8 minutes per session, significantly longer than the 3.0-minute average for standard interfaces. When these assistants incorporate personalized learning curves that adapt to individual digital proficiency levels, user retention increases by 41.5% over a six-month period. Notably, virtual assistants employing natural language understanding calibrated for older adults' communication patterns have achieved comprehension accuracy rates of 85.2%, compared to 72.4% for standard language models when processing financial queries from users over 65 years of age [9].

5.2. Personalized Guidance Through Financial Transactions

Personalized AI guidance systems have proven effective in supporting elderly users through complex financial transactions. Research shows that step-by-step transaction walkthroughs reduce error rates by 62.4% compared to standard banking interfaces. Systems incorporating real-time explanation of financial terminology have been particularly successful, with users reporting a 54.8% increase in confidence when completing online banking tasks. Longitudinal studies demonstrate that personalized guidance systems lead to a 36.7% increase in independent financial task completion over a three-month period. The integration of fraud detection components within these guidance systems has shown promise, with early implementations identifying potential scams with 81.3% accuracy and reducing successful fraud attempts against elderly users by approximately 40.2% compared to control groups using standard banking interfaces [10].

5.3. Building Digital Confidence Through Supportive Technology

Supportive AI technologies specifically designed to build digital confidence have emerged as a critical component of financial education for elderly users. Interactive learning modules incorporating financial concepts have demonstrated particular effectiveness, with completion rates of 71.5% compared to 30.8% for traditional educational methods. Systems providing positive reinforcement for successful task completion increased user confidence metrics by 42.9% over eight weeks of regular use. Research indicates that technologies incorporating social learning elements, including peer group support facilitated by AI moderators, improve knowledge retention by 37.6%. Additionally, support systems providing on-demand assistance through multiple channels (voice, text, and video) have been shown to reduce technology abandonment rates by 56.4%, significantly extending the duration of active engagement with digital financial services [9].

5.4. Measuring Effectiveness of AI Educational Interventions

Comprehensive measurement frameworks have been developed to assess the effectiveness of AI-based financial education interventions for elderly users. Quantitative assessments demonstrate that participants in AI-guided financial education programs show average improvements of 42.7% in financial literacy scores compared to baseline measurements. Behavioral metrics indicate a 35.9% increase in digital financial service utilization following structured AI interventions. Long-term tracking reveals that 66.5% of users maintain improved financial behaviors six months after completing educational programs, significantly higher than the 27.8% retention rate observed with traditional financial education methods. Cost-benefit analyses suggest that AI-assisted financial education programs deliver approximately $3.15 in prevented fraud losses and improved financial decision-making for every $1 invested in program implementation, making them particularly valuable for organizations serving vulnerable elderly populations [10].

6. Future Trends

6.1. Balancing Protection with Autonomy and Dignity

The implementation of AI-based protective systems must carefully balance security objectives with respect for individual autonomy and dignity. Research indicates that systems prioritizing user control report 56.8% higher satisfaction rates among elderly users compared to more restrictive approaches. Studies examining the psychological impact of protective technologies found that implementations preserving decision-making agency resulted in 41.5% lower rates of technology abandonment. Notably, systems incorporating graduated intervention protocols, where protective measures intensify only as risk increases, demonstrated optimal outcomes with 82.7% of users reporting feeling both protected and respected. Survey data shows that 77.4% of users prefer having the ability to override automated protections in non-critical scenarios, though this preference decreases to 34.6% for high-risk financial transactions exceeding personalized thresholds. These findings underscore the importance of designing systems that protect vulnerable users while maintaining their sense of independence and self-determination [11].

6.2. Transparency Requirements for AI Protective Systems

Transparency has emerged as a critical requirement for effective and ethical AI protective systems. Research demonstrates that explainable AI implementations result in 62.5% higher trust ratings compared to less transparent alternatives, with trust scores directly correlating with system adoption rates. Studies of disclosure practices found that comprehensive explanation of data collection practices improved user comfort levels by 46.3% compared to minimal disclosure approaches. Multi-modal explanation methods, combining visual, textual, and interactive elements, have proven particularly effective, with comprehension rates of 71.8% compared to 47.5% for text-only explanations of system functionality. Additionally, real-time notification of protective interventions, when delivered with clear

rationales, reduced user frustration by 37.6% compared to delayed or unexplained interventions, highlighting the importance of transparent communication about system actions [12].

6.3. Building Effective Partnerships Between Technology, Finance, and Social Services

Cross-sector collaboration has demonstrated significant potential for improving outcomes in protective technology implementation. Integrated approaches involving financial institutions, technology providers, and social service organizations have shown 50.7% higher effectiveness rates in preventing financial exploitation compared to single-sector solutions. Organizations implementing formal collaboration frameworks reported identifying 46.9% more potential cases of financial exploitation, with improved intervention outcomes in 67.5% of cases. Research indicates that multi-stakeholder governance models, where diverse experts share oversight responsibilities, result in systems that more effectively balance security and usability, with 43.2% fewer reported issues related to false positives or unnecessary restrictions. Implementation analysis has found that successful partnerships typically involve shared data standards, with interoperability increasing case resolution rates by 37.8% and reducing response times by 41.6% compared to siloed approaches [11].

6.4. Future Research Directions and Policy Recommendations

Analysis of current implementation challenges has highlighted critical areas for future research and policy development. Studies of regulatory frameworks have found that jurisdictions with specific AI governance standards report 35.9% higher rates of responsible technology adoption compared to regions with less developed guidance. Research priorities identified through multi-stakeholder consultations include improving algorithmic fairness for underrepresented populations, with current systems showing accuracy disparities of up to 17.8% between demographic groups. Policy assessments indicate that regulatory approaches emphasizing outcomes rather than specific technologies demonstrate 41.7% greater adaptability to rapid technological change. Prospective economic analysis suggests that standardized ethics frameworks could reduce implementation costs by 26.9% through decreased duplication of evaluation efforts. Furthermore, research supports extending existing financial consumer protection frameworks to explicitly address AI systems, with 73.5% of experts advocating for adaptations of current regulations rather than entirely new frameworks [12].

Table 1 Implementation Metrics for Ethical AI Protection Systems [11, 12]

Implementation Area	Metric	Value
User Autonomy	Users preferring override ability in non-critical scenarios	77.4%
Transparency	Improvement in comprehension with multi-modal explanations vs. text-only	24.3%
Multi-stakeholder Governance	Reduction in false positives with diverse expert oversight	43.2%
Regulatory Impact	Increase in responsible technology adoption with specific AI governance standards	35.9%
Cost Efficiency	Potential implementation cost reduction through standardized ethics frameworks	26.9%

7. Conclusion

The integration of AI technologies for protecting elderly individuals from financial fraud represents a promising approach to addressing a significant and growing societal challenge. This article has demonstrated how various technological interventions—from transaction monitoring to communication screening, predictive modeling, and educational support—can work in concert to create comprehensive protection systems. Critical to the success of these implementations is finding the appropriate balance between security objectives and respecting the autonomy and dignity of elderly users. The article underscores the importance of transparency in AI systems, the value of multi-sector collaboration between technology, finance, and social services, and the need for adaptive regulatory frameworks that can evolve alongside technological advancements. As these systems continue to develop, attention must be directed toward ensuring algorithmic fairness, standardizing ethical frameworks, and extending existing financial consumer protection regulations to address the unique challenges posed by AI-based systems. By addressing these considerations while continuing to refine the technological approaches outlined in this paper, we can work toward creating a safer financial environment for vulnerable elderly populations without compromising their independence or dignity.

References

[1] Federal Bureau of Investigation, "Elder Fraud Report 2022," Internet Crime Complaint Report, 2022. [Online]. Available: 2022_IC3ElderFraudReport.pdf

[2] Monica Anderson and Andrew Perrin, "Technology Use Among Seniors," Pew Research Center, 2017. [Online]. Available: Technology use among seniors

[3] Rahul Roy Devarakonda, "Machine Learning Approach for Fraud Detection in a Financial Services Application," IJSAT23012878, Volume 14, Issue 1, 2023. [Online]. Available: IJREAM-Approved By UGC

[4] Rabindra Jena, "Factors Impacting Senior Citizens' Adoption of E-Banking Post COVID-19 Pandemic: An Empirical Study from India," ResearchGate, 2023. [Online]. Available: (PDF) (PDF) Factors Impacting Senior Citizens' Adoption of E-Banking Post COVID-19 Pandemic: An Empirical Study from India

[5] J.T. Hancock, "Digital Deception: The Practice of Lying in the Digital Age," Social Media Lab, Stanford University, 2009. Digital Deception: The Practice of Lying in the Digital Age | Social Media Lab

[6] Om Uskaikar et al., "Multi-Modal Deception Detection Using Deep Learning," IEEE Conference Publication, IEEE Xplore, 2024. Multi-Modal Deception Detection Using Deep Learning | IEEE Conference Publication | IEEE Xplore

[7] Maria Casimiro et al., "Self-adaptive Machine Learning Systems: Research Challenges and Opportunities," SpringerLink, 2022. Self-adaptive Machine Learning Systems: Research Challenges and Opportunities | SpringerLink

[8] Emilija Strelcenia and Simant Prakoonwit, "Improving Classification Performance in Credit Card Fraud Detection by Using New Data Augmentation," MDPI, 2023. Improving Classification Performance in Credit Card Fraud Detection by Using New Data Augmentation

[9] Siwen Liu and Sharon, "Developing a Framework of Guiding Interface Design for Older Adults," SAGE Journals, 2012. Developing a Framework of Guiding Interface Design for Older Adults - Siwen Liu, Sharon Joines, 2012

[10] KangJie et al., "AI Literacy Education for Older Adults: Motivations, Challenges and Preferences," CHI EA '25: Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, 2025. AI Literacy Education for Older Adults: Motivations, Challenges and Preferences | Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems

[11] Stella R. Taquette et al., "Ethical Dilemmas in Qualitative Research: A Critical Literature Review," SAGE Journals, 2022. Ethical Dilemmas in Qualitative Research: A Critical Literature Review - Stella R. Taquette, Luciana Maria Borges da Matta Souza, 2022

[12] G. Abord-Hugon Nonet et al., "Multi-stakeholder Engagement for the Sustainable Development Goals: Introduction to the Special Issue," Springer link, 2022. Multi-stakeholder Engagement for the Sustainable Development Goals: Introduction to the Special Issue | Journal of Business Ethics

[13] Sanchayan Chakraborty, "Safeguarding seniors: How Network Security and AI Prevent Elder Fraud" IJSRCSEIT, 2025.

[14] Safeguarding seniors: How Network Security and AI Prevent Elder Fraud | Internation.al Journal of Scientific Research in Computer Science, Engineering and Information Technology