International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

AI in Fraud Detection for Elderly People- Preventing Scams against Elderly People

Reshma Sudra

Email: *sudra. Reshma[at]gmail.com*

Abstract: ***The fraudulent actions are elevating year by year in the technological world. It is crucial to identify such scam action for all the demographic populace from young adults to the elderly populace. The frauds are targeting senior citizens as they are weakened both physically as well as psychologically. It is performed mainly by trusted persons and with the intention of malicious actions. It is exemplified in the form of text or e - mail phishing, fake news, gambling or romance scams, investments or cryptocurrency scams, and health or consumer fraudulence. The fraudulent actions are prevented using the employment of AI techniques. It has the potential to identify spam calls or text messages and provide alertness which minimizes the risk of financial losses. Several digital fraudsters are more skillful and evaluate the loopholes and thereby develop cunning techniques such as phishing and wittingly money the unsuspected victims. Senior citizens are more vulnerable to such malicious actions and face economic losses. The present study analyses the financial threats to senior citizens and it overviews the modifications of the senior citizens in the emotional, biological, and psychological states. Moreover, the significance of AI techniques is discussed elaborately. The differential framework of AI is proposed and their beneficiaries are listed. Additionally, the mitigation strategies are proposed to distinguish spam from the senior populace thereby providing a secure digital environment. The present study contributes to the precious senior citizens by enabling them to live in a comfortable digital era.***

Keywords: AI, elderly populace, fraudulent actions, mitigation strategies, digital environment

1. Introduction

1.1 Background of the study

The digital age has been accompanied by extraordinary convenience and ease of access to financial transactions. It also brought novel challenges and the significant is an unremitting threat of fraudulent actions (Reurink, 2019) . The complexity and the volume of the transaction arise and fraudsters adapted their method and turned to be more sophisticated than before (Hashim, Salleh, Shuhaimi, & Ismail, 2020) .

Financial exploitation is a significant concern among elderly people and it severely impacts the growing segment of the populace in the industrialized nations (Coombs, 2014) . It will harm the senior citizens hugely. Financial exploitation is defined as the misuse or illegal utilization of the elderly person's assets, funds, and properties. It is performed mainly by trusted persons and with the intention of malicious actions. It is one of the forms of elder maltreatment (Burnes et al., 2017) . This financial fraudulence affects elderly people both emotionally and financially and elevates their dependence on them, reducing well - being, and penurious living conditions. It leads to a high rate of hospitalizations, poor mental and physical health, and finally morbidity and mortality (Carey, Hodges, & Webb, 2018) . People from all age groups can be scammed and older adults are exposed to scams comparatively to the young populace.

Perpetrators of the financial abuse are utilizing a variety of weapons against the elderly people. They also use psychological influences, and exploitation tactics that include manipulation, coercion, and deception to control the adults mentally (DeLiema, Deevy, Lusardi, & Mitchell, 2020) . There are several risk factors for older people to be exposed vulnerably to fraudulence and dependence on other people for financial actions, social isolation, reduced decision - making potential, and lack of experience in digital technologies. Moreover, the socio - emotional, cognitive, and neurobiological variations also contribute to the old age for the exploitation of financial assets.

Deception is the most common technique utilized in the exploitation process. Deception relies on lie detection in the interpersonal communication process (Ebner et al., 2020) . The differentiation of the truth and lie tellers is identified (Bailey, Taylor, Kingston, & Watts, 2021) . Deceptive context is a complex and diversified process and is established in the life domains. It is exemplified in the form of text or e - mail phishing, fake news, gambling or romance scams, investments or cryptocurrency scams, and health or consumer fraudulence (Burton, Cooper, Dar, Mathews, & Tripathi, 2022) .

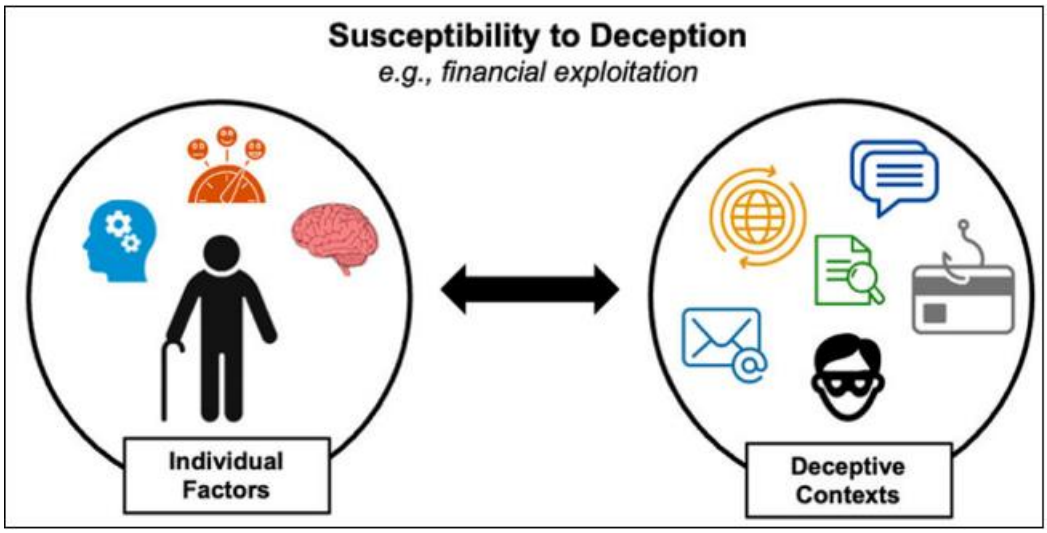

Figure 1: Conceptual framework of individual factors and deceptive context

Figure 1 illustrates the individual factors impacting the psychological risk factors and modification of the deceptive context contributes to the detection of deception and mediates the exploitation effectiveness. Modern spam makes use of the reciprocation influences and life domain finances in e - mail spam. The reciprocation is a significant influence weapon among the older adults and it is followed by appealing words such as soon - to - expire and limited offer. These words attract old age adults and motivate them to indulge in financial abuse.

Some of the scams are not revealed publicly due to embarrassment, loss of independence, and lack of awareness of elderly people. The tailored fraudulent scams impact the older adults which pave the way to provide special attention to that particular populace and thereby prevent them from such scams. Government policymaking, consumer protection entities, and law enforcement are some of the protective measures against spam (Cross, 2022) .

To resolve the challenges of cyber security in elderly people, AI - enabled support systems are proposed. It is a set of algorithms that monitors the incoming data and prevents fraudulent threats before processing them. The historical fraud data are reviewed by AI and detect and prevent such threats where the current software cannot have the potential to do such things (Alzahrani & Aljabri, 2022) . It is dynamic and progressively works to minimize the false positive threats and block them. The optimal cyber security is lightweight and it does not impact the website performance in the system.

1.2 Problem identification

In the statistical report of the European Union, it has been predicted that the elevation of scam rate among elders from 20% in 2019 to 30% in 2070. The low fertility rates and rising life expectancies are the chief reasons for the greater old age populace. The demographic variation also elevates the financial exploitation likely frauds. Numerous investigators reveal that the old - age populace is more vulnerable to fraudulent risks. The social, economic, and physical factors influence the old age populace subjected to the financial threat. The minimization of cognitive capacities reduced financial decision - making potential, and less technological guidance are the significant risks of senior citizens victimized by scams.

The economic status both in terms of wealth as well as assets attracts the frauds to target them. The higher personal wealth accumulation compared to young adults is also a factor impacting them. In terms of social factors, isolation in society might pave the easy way to manipulate them, and reduced awareness of financial scams also prone senior citizens to the victimization of fraudulent risks. Therefore, the present study attempts to provide the significance of AI - enabled support systems in the fraudulent detection among the elderly populace. Finally, it leads to the prevention of scams against them and providing safety environment for the senior populace of the nation.

1.3 Research question

The research questions of the present study are as follows:

1) What are the beneficiaries of utilizing AI among the elderly populace in the nation?
2) What are the threats faced by elderly people in digital transactions?
3) Whether AI can resolve the issues of fraudulent detection?
4) Illustrate the mitigation strategies for scam prevention among the old - age populace.

1.4 Objective

1) To overview the utilization and beneficiaries of AI among elderly people in the nation
2) To identify the diverse security threats faced by the elderly populace
3) To evaluate the impact of AI in the detection of financial fraudulent and prevention strategies
4) To recommend the mitigation strategies for scam prevention and provide a safe environment to the old age populace

1.5 Significance of the study

As technology rapidly grows, the digital divide differentiates the aging groups and young populace both physically and

digitally. The generations are immersed in technology further worsens the situation. It is difficult to connect and communicate with the older adults. The lack of technological knowledge and distrust of the technologies make the aging lovable populace to financial threats. According to the FBI Internet Crime Complaint Center, 2022 Elderly Fraud report, the elders are subjected to scam victimisation and states that the 300% elevation in the monetary losses in the year 2021 - 2022. And a 350% increase in the reported losses due to cryptocurrency scams.

AI - enabled supporting systems aid in detecting financial threats and combating their trends and finally reducing the risk of financial losses and reputation destruction. It can able to differentiate the messages of trusted people and malicious threats. It has the potential to detect fake accounts and thereby prevent the threats caused by them. Multi - factor authentications are utilized in AI to prevent account takeover. The credential stuffing attack will be pre - determined using AI tracking of the traffic sites and high login failure rates demonstrate that the particular account is under the attack.

Moreover, AI can process and block financial threats in a fraction of a seconds. It provides excellent security in terms of dynamic and speed. It is cost - effective to eradicate the financial losses of the elderly populace and safeguard them both physically and mentally. Therefore, the present study attempts to overview the financial threats of the old age populace and recommend the AI system to prevent such risks. The framework of the AI system provides an excellent pathway to minimize financial exploitation and safeguard the precious experienced senior citizens of the nations.

1.6 Paper Organisation

The paper is organized in the following sequential manner. Section 1 illustrates a brief introduction regarding the impact and significance of AI in fraudulent detection among elderly people. It also depicts the significance of research. Section 2 describes the prevailing scholarly research works related to the present research. Section 3 provides a detailed analysis of financial threats and beneficiaries of AI and its mitigation strategies. Section 4 illustrates the discussion as well as the limitations of the study. Lastly, section 5 discusses the conclusion and future recommendations of the study.

2. Literature Review

The existing study (Saumya & Singh, 2018) discusses the AI tool in debunking digital spam reviews in the online platform. It is considered to be a trustworthy tool and two major types were categorised. They are the Text tool and Behavioural tool. The text tool inaugurates the detection criteria and it is associated with the textual features of the criticism. The Behavioural tool inaugurates the detection criteria associated with the behavioral features. The older adults and younger ones trust the AI tool and modify the credibility judgments for the total attitude and reviews towards the products marketed by them. AI tools are utilized to measure the originality of the reviews. It has been found that older adults trust the AI tools and up to 48% of the fraudulent are detected by the AI and their risky judgments are demolished. Alternatively, younger adults have high trust in the behavioral tool compared to the textual tool. The behavioral tool identifies more spam reviews by themselves. The AI tools are perceived to be more competent as well as benevolent where AI outstripped the participants through the identification of unexpected spam reviews.

The prevailing study (Xue, Wang, Luo, Seo, & Li, 2019) demonstrates the elevated popularity of the digital review systems. The huge information of the user aids the people to review more about the service quality and product guarantee from unknown firms. These review platforms are frequently utilized by capable malicious users with the absence of validation. These review system targets older age adults and includes deceptive reviews by manipulating the content and rating of the reviews (Xue & Li, 2017) . The existing study proposes an AI spam detection framework to segregate the aspect - oriented reviews and aggregated opinions on the appropriate aspects. The impact on the loyalty of the user because of their opinion differences and combining the penalties to generate the trust scores for reviews, users, and targets appropriately. The potential indicators of fraudulence are the trust scores because they reflect the deviation of the opinion on particular aspects. The existing study gathers the dataset from Yelp. com and reveals that the proposed detection system aids in finding out the user's loyalty based on the opinions expressed in the feedback system.

The prevailing study (Soni, 2019) discusses the fraudulence activities in financial institutions that target elderly clients. The transaction data in the accounts of the chief financial institutions are tracked and the identification of malware actions in the elder clients' accounts. It has been analyzed on the data comprising of 5 million accounts for the client possessing age of 70 years and above. Almost 250 million transactions are performed in the period of 2015 January to 2016 August. The significant focus is to improve alert detection through the utilization of the transaction monitoring techniques. The random forest, logistic regression, and vector ML techniques are utilized for the detection frameworks. The integration of the techniques with the correction of the imbalances in alertness paves the way to generate a novel framework. This novel framework aids in providing an alert system for the protection of elder clients in significant institutions. The findings reveal the impact of the client traits and activity of the accounts in the selection of the fraudulent alert prototypes.

Multiple techniques were utilized in the research to determine the effective working model for distinguishing deceitful money transfers, which was laid out utilizing the precision of the model, and the hustle in identifying the expense (Jeevan, Naresh, & Kambli, 2018) . Therefore, several models were used which included the Bayesian network, KNN, Neural network, SVM, and other supplementary. A comparison table used in this research provided the most accurate and efficient network in dealing with fraudulent transactions was the Bayes - Ian Network. The other model of KNN performed excellently, and the recognition was quick, with mediocre precision, through the KNN's haste was great, with a medium exactness. Finally, it is mentioned a lower score in SVM, speed relates to it slow than others, and medium precision existed. Concerning the expense, all models assembled were sweeping.

The prevailing study (Malini & Pushpa, 2017) proposed that involving KNN as outlier detection in distinguishing card misrepresentation as creators found in the wake of playing out their model over examined information, that the fittest technique in recognizing and deciding target instance irregularity in KNN, which showed that its most fit in the detection of extortion with the memory restriction. Concerning anomaly identification, the calculation and memory expected for the charge card extortion recognition is substantially less, not its functioning quicker and better in enormous web - based datasets but KNN was more exact and effective than the results shown in the study. Further, a model that was used for SVMs and valued the brain frameworks was made. In this assessment, three - layer feed - forward RBF neural frameworks associated with recognizing counterfeit charge card trades, through only two passes are expected to create a distortion score predictably.

In today's world, numerous Artificial Intelligence techniques are developed. The existing study (Makki et al., 2019) describes that credit card fraud causes huge financial losses. Most of the researchers have been employed on this to provide an advanced way to eliminate this loss and most of the available approaches are costly, time - consuming, and labour - incentive tasks. The research has found that the imbalanced classification of the dataset is the main reason for the inaccurate results after many experimental studies. These imbalance classifications consist of the unbalanced dataset, which caused the model to predict inaccurate and cause financial loss. Therefore, they have found that LR, C5.0 decision tree algorithm, and considered SVM and ANN are the best algorithms based on accuracy and AUCPR for sensitivity. They have used the balanced dataset to train these models.

Further, (Sadgali, Sael, & Benabbou, 2021) work describe that nowadays banking transactions like online transactions, credit card transactions, and mobile transactions, etc. are gaining popularity because all people prefer digital and paperless transactions and millions of transactions carried out and all them subjected to a type of fraud. Many of the researchers have analyzed, designed, and developed a model for detecting fraud using machine learning. They presented a comparison among the entire machine - learning algorithm to select which model is best for fraud identification in card transactions.

To explain more (Karthik, Mishra, & Reddy, 2022) proposed a misrepresentation location framework with non - overlapped risk - based bagging ensemble (NRBE) model to deal with the uneven dataset and to keep away from the noisiness contained in the transactions. The model breaks all the irregularities in the dataset and its non - vital nature. The sacking model is reached out by a pack of creation and danger - based base students. The bag creation eradicates the problem faced by imbalanced data and Naïve Bayes destroys the issue brought about by noisiness created in the transactions. The proposed model has been beaten with 5% in BCR and BER, half of the recall, and 2x or 2.5x decreased expense to fraud detection by utilizing the NBRE. It was observed that the NRBE model is best suited for fraud detection and it is most appropriate for business dynamic technique.

The existing study (Ryman - Tubb, Krause, & Garn, 2018) discusses AI and ML research and its impact on payment card fraudulent detection techniques. The objective of the research study is to guide the research community to better transit the research into the fraudulent detection in the credit card system. Payment card fraud is a complex and serious threat to the society. It involves the identification of financial terrorism. The fraud pattern slowly evolves and the criminals remain unsophisticated. The evolution of disruptive technologies likely smartphones, cloud computing, and mobile payments emerged simultaneously with the huge data breaches. This led to the development of new fraud vectors compared to the less effective conventional techniques. Conventional research signifies the utilization of ML and AI in fraudulent detection techniques and proposes that cognitive computing are promising research guidance that enhances data philanthropy.

2.1 Research Gap

1) The existing study (Saumya & Singh, 2018) focuses on the research of AI tools rather than the algorithms, hence the outcome might be biased. Moreover, the sample populace is homogenous which lacks generalizability in the results.
2) The conventional study (Xue et al., 2019) proposes a framework where the data labeling process is tedious and time - consuming. The data labeling is also limited.
3) The existing study (Ryman - Tubb et al., 2018) proposes guidance for the minimization of fraud in credit cards. It failed to propose a framework for the detection system.

3. Fraudulent detection

3.1. Overview of financial threats

The variation in psychological well - being is pre - determined utilizing economic soundness. Poor psychological, sleep disruption, and decline in mental health impact the low economic soundness. Figure 2 illustrates the modifications faced by the elderly populace that affect their psychological well - being.

- **Biological modification**

It involves the variation in physical health due to breathing functions, high pressure, and blood stroke. The biological modification influences the psychological well - being of the old - age populace.

- **Cognitive modifications**

It arises due to the damage in the nerve cells and constitutes the decline in reminiscence, Parkinson's disease, and Alzheimer's disease. It provides anxiety feelings to the populace and minimizes their mental health status

- **Social modifications**

The elders are facing issues in completing the day - to - day chores. Additionally, they lack access to healthcare facilities and are required to depend on others for activities. They do lack mental fitness.

- **Emotional modifications**

The destruction in both their mental and physical well - being impacts them and transforms them into more dependent on others. The loneliness engages them and feel helpless.

In addition to the above modifications, economic soundness also plays a significant role in the psychological well - being of the old - age populace (Qian, Zhang, Yamamoto, & Schuller, 2021) .

AI utilized by fraudsters

AI can elevate the volume as well as the sophistication of scams and frauds. There has been a report conveying the three million cases of AI fraudulence in the UK in the year 2022. AI content in the form of text and images is not easily discernible from human - generated content without the utilization of specialized tools (King, Aggarwal, Taddeo, & Floridi, 2020) . There are no standardized procedures to reveal that AI is not utilized by fraudsters.

Biological Modifications	Cognitive Modifications	Social Modifications	Emotional Modifications
• The inner modifications that arise within the frame include alternate in-frame mass, a decline in breathing function, down flip in the kidney and aerobic vascular system, osteoporosis, hearing loss, visible deterioration, continual body aches, diabetes, high blood pressure, and stroke, etc.	• Cognitive modifications arise because of harm to the nerve cells in the brain and they constitute to the reminiscence decline, dementia, Alzheimer's disease, Parkinson's disease, melancholy and anxiety etc. - M. Felez-Nobrega, J.M. Haro, (2022), Lisa Engel, Yael Bar, et.al., (2016).	• Elders have problems completing their everyday chores, limitations to accessing health care and fitness and health coverage, the lack of the life of a cherished one, and end-of-existence preparation- Srivastava, S., et al., (2021).	• The decline in fitness both physically and mentally makes the aged turn out to be extra dependent, sense lonely, disregarded, financially constrained, have attachment needs, and helpless - Kenneth F. Ferraro, Ya-ping Su, (1999).

Figure 2: Modifications impacting the psychological status

AI is generally utilized to produce fake content and generate malicious user profiles. There are six main ways to perform the scam among the elderly populace. Volume and sophistication are two main dimensions that elevate fraud.

- Volume amplifies the potential of fraudsters through the generation of scam context at the greater levels
- Sophistication elevates the rate of success through the generation of personalized and convincing scam content.
- Moreover, the third dimension is time which reveals that the AI potentials are evolving rapidly with the fraudulent usages.

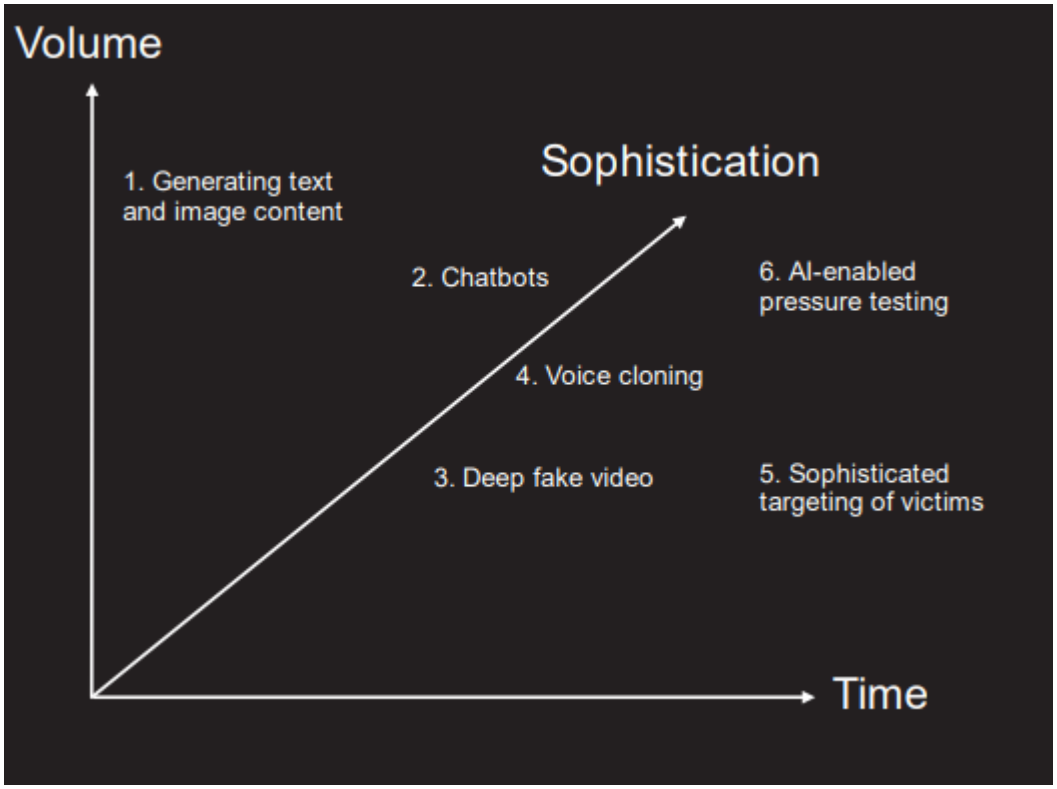

Figure 3: AI in deploying the perpetrate of scams and frauds (King et al., 2020)

Figure 3 illustrates the utilization of AI in exhibiting scams and fraudulent actions to the elderly populace. It supports generating the text and image content of malicious actions that attract the user to indulge in such activities. Another is Chatbot, where the messages are resembled as trusted persons that influence the senior citizens. Fake video and voice cloning are the two major aspects conducted by digital fraudsters to attract the senior populace for fraudulent actions. The victims are targeted specifically in terms of age category as they are considered to be a weakened society. These are the stages in which fraudsters carry out malicious actions against senior citizens to cause financial threats (Sinha, Chacko, & Makhija, 2022) .

3.2 Benefits of AI in fraudulent detection

Frauds are common in financial transactions and encompass frauds in financial statements, money laundering, cyber frauds, and credit card frauds. Digital banking is also prone to digital fraud. Fraud management is essential for the financial transaction, even though it is considered an excruciating venture. The digital fraudsters are more skillful and able to identify the loopholes. They also develop cunning techniques such as phishing for the anonymous victims and deliberately extract money from them. It paves the way to generate detection procedures for fraudulence. It's time to devise a new technique that can bypass conventional and rigid security protocols. It also learns to convince the unsuspected phone calls. Conventional fraud detection techniques are unsustainable and unsalable and experienced hackers can overcome the conventional detection techniques. Adding the challenges to the traditional system, the hackers make use of advanced techniques to hack digital transactions.

Conversational AI

Machine learning will aid in detecting harmful content and eradicate them in the platforms. The online fraud charter makes use of advanced techniques, hence, preventive measures should be undertaken to demolish the fraud ecosystem. The anonymous call detection can be handled by the AI in the following system proposed in Figure 4.

The suspicious and unsolicited calls are deceptive and utilized by malicious users. It is a major issue faced by the senior citizens (Elizalde & Emmanouilidou, 2021) . It refers to scams or spam calls. It usually tricks the users into revealing personal information such as their passwords, financial data, and government identifiers. Fraudulent possess themselves as government officials and cause threats to older adults to gain their trust of them. They also asked to pay in a scammer's account. The scam detection in the conversation requires an understanding of the conversational flow at the appropriate time. The smartphone application detects such calls and identifies suspicious actions. AI detects such calls and alerts the users. The conversational AI has experienced scam call data sets and with the permission of the users, it analyses the anonymous calls in real - time to identify whether the call is suspicious. While it detects such calls, it alerts the user not to reveal sensitive information to such unknown numbers. Moreover, the conversational agent answers the call and performs the conversation with a scammer if the user permits them. It minimizes the frequency of spam calls. The conversational agents are trained in such a manner to resolve the novel strategy followed by the spam callers.

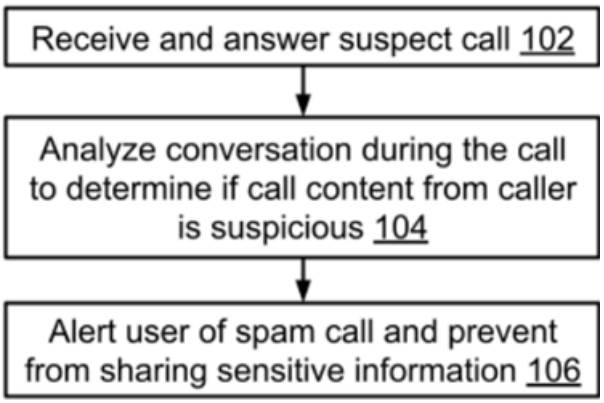

Figure 4: Conversational AI in the fraudulent detection

The above figure illustrates the detection of suspicious calls by the AI model. The conversational AI has been trained on the larger data sets to differentiate the spam as well as non - spam phone calls. When the call is received from unknown numbers, the calls are attended by a user or directly by the conventional agent based on user preferences. The conversations are analyzed in real - time to determine whether it is a scam or not. The audio might be converted into text and analyses whether the content matches the spam. The content aids in detecting the call pattern matches with the spam calls. Additionally, it also identifies textual scam messages in the form of cryptocurrencies, gift coupons, and messages from unknown contents. Options are also provided to the users in reporting the call as suspicious.

Trained AI offers numerous beneficiaries that minimize the burden of such calls and messages. It can handle the changing strategies of scammers. These techniques can be easily accessible to all management systems as it is reliable and stable. Therefore, conversational AI secures senior citizens in providing a safe digital environment and enables them to live in a comfortable zone.

Generative AI

It is a backbone and utilises the deep neural network and the chief example is Chat GPT. It is constructed to reveal a data sequence in the output generation and trained through the sequential data likely payment sentences and histories. It distinguishes whether the technique is fraud or not based on training provided on the input data. It can progress indefinitely and is considered to be a superlative tool for generating the data on the actual data (Veloso, Balch, Borrajo, Reddy, & Shah, 2021) .

The following tools in detection of the fraudulence are

- Logistic expressions
- Decision trees
- Random forest
- Deep learning
- Natural language processing

Logistic expression is the supervised learning technique that is established by decisions. The acquired results distinguish as non - fraud as well as fraud in the initial transaction process. It is a complex technique and it handles huge variables (Langevin, Cody, Adams, & Beling, 2022) . It is a reliable method of detecting the fraudulent. Alternatively, in the random forest technique, the AI generates a graphical representation of the decision - making process. The algorithm identifies the crucial variables and proposes a framework for the detection process. It discards the unrelated features and does not require a huge data. Another technique is a random forest which integrates the decision trees to generate more results. It has fast runtime and the ability to handle missing data. Neural networks are constructed based on human brains. It utilizes cognitive computing which supports the development of machines that utilize self - learning algorithms. It is fast as well as functions in real - time. A master card prevents the card - associated funds. The outcomes are impressive and minimize the fraudulent practices. NLP extracts the signals from the IVR voices, interactions as well and chats to support the senior citizens in preventing suspicious actions in financial transactions.

3.3 Mitigation Strategies

Through the utilization of advanced algorithms, the AI system can identify the disrupted patterns that indicate the suspicious actions. It is a potential detection system that learns from previous interactions and enhances the predictive capabilities in real time (Samtani, Kantarcioglu, & Chen, 2020) . It is constructed in such a way to evaluate and interpret the complex data. It enables them to reveal the hidden pattern as well as anomalies that identify the fraudulent actions. The ML, NLP, data analytics, and AI systems process huge volumes of both unstructured as well as structured data (Găbudeanu, Brici, Mare, Mihai, & Șcheau, 2021) . It assesses the outliers and produces actionable insights over time. This approach empowers the senior citizens to evaluate the fraudulent actions in the earlier phase and execute optimal mitigation strategies.

The mitigation strategies provided by AI are as follows:

a) Unraveling transactions
AI algorithm aids in monitoring digital transactions and identifies suspicious activities. The algorithms assess the historical data, user behavioral features, and contextual data to detect deviation from the original patterns. It can able to flag transactions that are above the typical spending habit of the user and exhibit differential geographical locations. It provides alertness to the senior citizens about the fraudulent actions.

b) AML – Anti - Money Laundering
It is a revolutionizing process that augments the conventional rule - associated systems with the aid of advanced analytics. It can analyze huge amounts of data extracted from various sources likely user profiles, transaction records, and data feeds in external, and identify the patterns that indicate the AML actions (Ashtiani & Raahemi, 2021) . AI can improvise the senior citizens to evaluate the complex laundering schemes minimising the false positives and improve the efficiency of AML.

c) Verifying the identities
AI algorithms are utilized globally to reinforce identity verification systems. The biometric authentication and facial recognition are powered by the system that enables to identification of the customer identity more effectively. It compares the facial features, assesses the ID documents, and validates the information to identify fraudulent actions.

d) Cyber security

It plays a significant role in the strengthening of the cyber security measures. It can analyze the network traffic and identify the pattern of suspicious actions. It can detect potential threats in real - time. It improvises fraud prevention through identification as well as neutralizing emerging threats. It minimizes the risk of financial losses and data breaches.

e) Ethical considerations

AI generates immense potential in fraudulent detection and risk management systems. The transparency, ethical use, and fairness of the AI algorithms should construct trust and aid in mitigating the risk related to the decision - making process automatically.

f) Looking ahead

The digital world evolving rapidly and AI plays a dominant role in fraudulent actions and risk management. Advanced technologies such as network evaluation, and DL aid in identifying fraudulent actions accurately. The collaborative efforts amongst AI experts and users are essential in leveraging the maximum potential of AI in regulating the greater standards of ethics and security.

4. Discussion

The present study focuses on the scams faced by the elderly populace and the role of AI in detecting fraudulent actions. The financial threats and challenges of senior citizens in digital transactions. The effect of deploying AI in minimizing risk strategies is discussed elaborately. The mitigation strategies are listed to mimic the suspicious actions.

The existing study (Xue et al., 2019) proposes an AI spam recognition framework to isolate the aspect - oriented reviews and aggregated opinions on the suitable aspects. The influence on the loyalty of the user because of their opinion modifications and combining the consequences to generate the trust scores for reviews, users, and targets appropriately. The potential indicators of deceitfulness are the trust scores because they reflect the deviation of the opinion on particular aspects. The existing study gathers the dataset from Yelp. com and reveals that the proposed detection system aids in finding out the user's loyalty based on the opinions expressed in the feedback system. Likewise, the current study discusses AI strategies for minimizing fraudulent actions among the elderly populace. It insists on differential AI technologies to identify spam calls and prevent them from financial threats.

Likewise, the prevailing study (Soni, 2019) demonstrates the fraudulence activities in financial organizations that target elderly clients. The transaction statistics in the accounts of the chief financial institutions are tracked and the documentation of malware actions in the elder clients' accounts. It concludes that the alertness of the firms to the clients will eradicate fraudulent actions. The present study also articulates the significance of conversational and generative AI tools in distinguishing normal and spam calls. It will alert senior citizens not to reveal sensitive information to anonymous numbers.

Similarly, the existing study (Ryman - Tubb et al., 2018) discusses AI and ML research and its impact on payment card fraudulent detection techniques. The evolution of disruptive technologies likely smartphones, cloud computing, and mobile payments emerged simultaneously with the huge data breaches. It concludes that cognitive computing are promising research guidance that augments data philanthropy. Likewise, the present research also signifies the evolution of AI in the digital World that mitigates the financial threat caused by fraud to the elderly populace.

4.1 Limitations

The chief limitation of the proposed study is it focuses on a particular populace of senior citizens. Hence, the results might lack generalizability. The outcome of the research does not apply to the universal populace and is restricted to the specific age category. However, the present study recommends that senior citizens utilize AI techniques to safeguard them from scams.

5. Conclusion

Nowadays, most people are using credit cards, money transfer services, and investing in stock market shares, due to which the number of fraudulent transactions is at a great height, and there is a need to develop the fittest AI techniques, which can address the intensifying problem. Further, fraudsters don't crack cards manually they use bots to perform the work for them, often brute force attacks can severely stain payment gateways. Whereas, for the money transfer fraudsters do fake account creation to skew your predictive reviews and make false requests to send money that was not authorized by a legitimate user and can be done on cards, which were illegally obtained. In today's world, new schemes have evolved that exploit investors to send money into fake accounts or identities such as romance scams, fake e - transfers, text messages, lottery, and sweeps, Get out of Jail, Guaranteed Loan. The elderly populace is greatly influenced by them and affected both physically and psychologically. It's a time to safeguard such a precious populace. Therefore, the present study analyses the financial threat of senior citizens and recommends the deployment of AI techniques to identify such threats and also demonstrates the mitigation strategies. The present study contributes to the senior citizens for providing a comfortable and safe digital environment in the technological era.

References

[1] Alzahrani, R. A., & Aljabri, M. (2022). AI - Based Techniques for Ad Click Fraud Detection and Prevention: Review and Research Directions. *Journal of Sensor and Actuator Networks, 12* (1), 4.

[2] Ashtiani, M. N., & Raahemi, B. (2021). Intelligent fraud detection in financial statements using machine learning and data mining: a systematic literature review. *IEEE Access, 10*, 72504 - 72525.

[3] Bailey, J., Taylor, L., Kingston, P., & Watts, G. (2021). Older adults and "scams": Evidence from the mass observation archive. *The Journal of Adult Protection, 23* (1), 57 - 69.

[4] Burnes, D., Henderson Jr, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the

United States: A systematic review and meta - analysis. *American journal of public health*, *107* (8), e13 - e21.

[5] Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental gerontology*, *159*, 111678.

[6] Carey, C., Hodges, J., & Webb, J. K. (2018). Changes in state legislation and the impacts on elder financial fraud and exploitation. *Journal of Elder Abuse & Neglect*, *30* (4), 309 - 319.

[7] Coombs, J. (2014). Scamming the elderly: An increased susceptibility to financial exploitation within and outside of the family. *Alb. Gov't L. Rev.*, *7*, 243.

[8] Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging. *Crime Prevention and Community Safety*, *24* (1), 30 - 41.

[9] DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2020). Financial fraud among older Americans: Evidence and implications. *The Journals of Gerontology: Series B*, *75* (4), 861 - 868.

[10] Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S.,. . . Spreng, R. N. (2020). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*, *75* (3), 522 - 533.

[11] Elizalde, B., & Emmanouilidou, D. (2021). *Detection of robocall and spam calls using acoustic features of incoming voicemails.* Paper presented at the Proceedings of Meetings on Acoustics.

[12] Găbudeanu, L., Brici, I., Mare, C., Mihai, I. C., & Șcheau, M. C. (2021). Privacy intrusiveness in financial - banking fraud detection. *Risks*, *9* (6), 104.

[13] Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). The risk of financial fraud: a management perspective. *Journal of Financial Crime*, *27* (4), 1143 - 1159.

[14] Jeevan, B., Naresh, E., & Kambli, P. (2018). *Share price prediction using machine learning technique.* Paper presented at the 2018 3rd International Conference on Circuits, Control, Communication and Computing (I4C).

[15] Karthik, V., Mishra, A., & Reddy, U. S. (2022). Credit card fraud detection by modelling behaviour pattern using hybrid ensemble model. *Arabian Journal for Science and Engineering*, 1 - 11.

[16] King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and engineering ethics*, *26*, 89 - 120.

[17] Langevin, A., Cody, T., Adams, S., & Beling, P. (2022). Generative adversarial networks for data augmentation and transfer in credit card fraud detection. *Journal of the Operational Research Society*, *73* (1), 153 - 180.

[18] Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M. - S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access*, *7*, 93010 - 93022.

[19] Malini, N., & Pushpa, M. (2017). *Analysis on credit card fraud identification techniques based on KNN and outlier detection.* Paper presented at the 2017 third international conference on advances in electrical, electronics, information, communication and bio - informatics (AEEICB).

[20] Qian, K., Zhang, Z., Yamamoto, Y., & Schuller, B. W. (2021). Artificial intelligence internet of things for the elderly: From assisted living to health - care monitoring. *IEEE Signal Processing Magazine*, *38* (4), 78 - 88.

[21] Reurink, A. (2019). Financial fraud: A literature review. *Contemporary Topics in Finance: A Collection of Literature Surveys*, 79 - 115.

[22] Ryman - Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, *76*, 130 - 157.

[23] Sadgali, I., Sael, N., & Benabbou, F. (2021). Bidirectional gated recurrent unit for improving classification in credit card fraud detection. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, *21* (3), 1704 - 1712.

[24] Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline: A multi - disciplinary research roadmap (Vol.11, pp.1 - 19): ACM New York, NY, USA.

[25] Saumya, S., & Singh, J. P. (2018). Detection of spam reviews: a sentiment analysis approach. *Csi Transactions on ICT*, *6* (2), 137 - 148.

[26] Sinha, M., Chacko, E., & Makhija, P. (2022). AI Based Technologies for Digital and Banking Fraud During Covid - 19 *Integrating Meta - Heuristics and Machine Learning for Real - World Optimization Problems* (pp.443 - 459): Springer.

[27] Soni, V. D. (2019). Role of artificial intelligence in combating cyber threats in banking. *International Engineering Journal For Research & Development*, *4* (1), 7 - 7.

[28] Veloso, M., Balch, T., Borrajo, D., Reddy, P., & Shah, S. (2021). Artificial intelligence research in finance: discussion and examples. *Oxford Review of Economic Policy*, *37* (3), 564 - 584.

[29] Xue, H., & Li, F. (2017). *A content - aware trust index for online review spam detection.* Paper presented at the Data and Applications Security and Privacy XXXI: 31st Annual IFIP WG 11.3 Conference, DBSec 2017, Philadelphia, PA, USA, July 19 - 21, 2017, Proceedings 31.

[30] Xue, H., Wang, Q., Luo, B., Seo, H., & Li, F. (2019). Content - aware trust propagation toward online review spam detection. *Journal of Data and Information Quality (JDIQ)*, *11* (3), 1 - 31.